

SME Server V5 with ServiceLink

User Guide - 5.1

Mitel Networks Corporation

SME Server V5 with ServiceLink: User Guide - 5.1

by Mitel Networks Corporation

Published January 2002

Copyright © 2002 by Mitel Networks Corporation

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with no Invariant Sections, one Front-Cover Text: "Not Endorsed by Mitel Networks Corporation", and one Back-Cover Text: "For the official SME Server V5 with ServiceLink User Guide, visit <http://www.e-smith.org/docs/manual/> (<http://www.e-smith.org/docs/manual/>)" Permission is granted for production of verbatim copies without the cover texts. A copy of the GNU Free Documentation License is available on our web site at <http://www.e-smith.org/docs/gfdl.html> (<http://www.e-smith.org/docs/gfdl.html>) and from the Free Software Foundation at <http://www.fsf.org/copyleft/fdl.html> (<http://www.fsf.org/copyleft/fdl.html>).

The Mitel logo and the terms "information bay" and "i-bay" are trademarks or registered trademarks of Mitel Networks Corporation in the United States and other countries. Linux is a registered trademark of Linus Torvalds. The terms "ssh" and "Secure Shell" are trademarks of SSH Communications Security Corp. Trend Micro is a registered trademark of Trend Micro Incorporated. All other trademarks are the property of their respective holders.

\$Revision: 1.157 \$

Table of Contents

1. Welcome to your SME Server V5 with ServiceLink	5
1.1. About This Guide.....	5
1.2. Software Licensing Terms and Conditions	5
1.3. About Our Test Company: The Pagan Vegan	6
1.4. What's New	6
2. The role of the SME Server V5	7
3. ServiceLink.....	8
4. Your Internet Service Provider (ISP).....	10
4.1. Dedicated versus dialup connectivity	10
4.2. The IP address.....	10
4.3. Arranging connectivity with your ISP	11
4.4. Arranging Services From Your ISP	13
5. Hardware Requirements of the SME Server V5 with ServiceLink Host Computer.....	17
5.1. Hardware Requirements for a Category 1 Server	17
5.2. Hardware Requirements for a Category 2 Server	18
5.3. Hardware Requirements for a Category 3 Server	18
5.4. Hardware Requirements for a Category 4 Server	19
5.5. Supported Ethernet Adapters	19
5.6. Supported SCSI Adapters	21
5.7. Supported Tape Drives	22
6. Installing And Configuring Your SME Server V5 with ServiceLink Software	23
6.1. Licensing Terms and Conditions	23
6.2. RAID1 Support (Disk Mirroring).....	23
6.3. Upgrading From A Previous Version.....	23
6.4. Installing the Software	24
6.5. Configuring your SME Server V5 with ServiceLink.....	24
6.6. Setting Your Administrator Password.....	25
6.7. Configuring Your System Name and Domain Name.....	25
6.8. Configuring Your Local Network	26
6.9. Operation Mode	27
6.10. Configuring Server and Gateway Mode.....	28
6.11. Server and Gateway Mode - Dedicated	29
6.12. Configuring the Server for Server and Gateway Mode - Dialup Access	31
6.13. Configuring Your DHCP Server	32
6.14. Further Miscellaneous Parameters.....	34
7. The Server Console.....	35
7.1. Using the Text-based Browser	35
7.2. Accessing the Linux Root Prompt	35
8. Configuring the Computers on Your Network.....	37
8.1. What Order to do Things	37
8.2. Configuring Your Desktop Operating System	37
8.3. IMAP versus POP3 e-mail.....	39
8.4. Configuring Your E-mail Application.....	40
8.5. Configuring Your Web Browser.....	41
8.6. Configuring Your Company Directory.....	41
9. On-going Administration Using the server manager	43
10. Security.....	44
10.1. Password	44
10.2. Remote Access.....	44
10.3. Local networks.....	46
11. Configuration	48
11.1. Set date and time.....	48
11.2. Workgroup	48
11.3. Directory	49
11.4. Printers	50
11.5. Hostnames and addresses.....	51
11.6. E-mail Retrieval	53

11.7. Other E-mail Settings.....	54
11.8. Review Configuration	55
12. Collaboration	56
12.1. User Accounts.....	56
12.2. Quota Management.....	57
12.3. Groups.....	57
12.4. Pseudonyms	58
12.5. Information Bays	59
12.6. Virtual Domains	59
13. ServiceLink.....	60
13.1. Status.....	60
13.2. Virus Protection	60
13.3. DNS Services	61
13.4. IPSEC VPNs	62
14. Administration	64
14.1. Blades.....	64
14.2. Backup or Restore.....	64
14.3. Reinstallation Disk.....	65
14.4. Mail Log File Analysis	66
14.5. View Log Files.....	66
14.6. Reboot or Shutdown	66
15. Miscellaneous	68
15.1. Online manual.....	68
15.2. Create Starter Web Site.....	68
15.3. Other Administration Notes.....	68
16. Information Bays (i-bays)	69
16.1. i-bay Directories.....	69
16.2. Accessing the i-bays	70
16.3. Creating an i-bay.....	70
16.4. Modifying an i-bay	71
16.5. An i-bay Used as a Customer Site: The Miles Gabriel Art Exposition	72
16.6. An i-bay Used as a Shared Network Drive	72
16.7. An i-bay Used as an Intranet: The Pagan Vegan "Vegemite"	73
16.8. An i-bay Used to Expedite Processes: Samson's Farms.....	74
16.9. An i-bay Used as Your Customer Download Site.....	75
17. User File Storage on the SME Server V5 with ServiceLink	77
17.1. Windows	77
17.2. Macintosh OS.....	78
18. Webmail.....	81
18.1. Enabling Webmail On Your System	81
18.2. Starting Webmail	81
18.3. Logging In.....	81
18.4. Viewing The Inbox.....	82
18.5. Logging Out of Webmail	82
18.6. Composing Messages.....	82
18.7. Reading Messages.....	83
18.8. Deleting Messages	84
18.9. Using Contacts.....	84
18.10. Changing Webmail Preferences	86
19. Additional Software.....	87
A. Introduction to the Ethernet Local Area Network (LAN)	88
B. Dynamic DNS Services	89
C. Proxy Servers	90
D. Technical Support.....	91

Chapter 1. Welcome to your SME Server V5 with ServiceLink

Congratulations on choosing the SME Server V5 with ServiceLink as your network and communications server!

Companies all over the world are using the Internet to communicate more effectively and efficiently to a broader audience. The SME Server V5 with ServiceLink is founded upon state of the art technologies - such as the Linux operating system - which have been mainstays in the infrastructure of larger organizations for several years. Mitel Networks Corporation has customized these technologies to make them straightforward to use, while still giving you local control over your Internet services. The result is a cost-effective Internet infrastructure that will reliably serve your organization as it grows and as its use of the Internet evolves.

For a list of authorized resellers or more information about support options, reseller programs and the worldwide community of SME Server developers and customers, please contact us at +1-613-564-8000 (in the the U.S. or Canada, please call 1-888-376-4841), or visit our website, <http://www.e-smith.com/>.

1.1. About This Guide

This user's guide walks you step-by-step through the straightforward process of installing and configuring your SME Server V5 with ServiceLink. The Appendices in the back of the guide provide background information on subjects related to networking and the Internet and are intended to supplement chapters in the main section of the user's guide.

1.1.1. Production

We created this user's guide using Docbook (<http://docbook.org/>) on the Linux operating system. Images were created using The GIMP (<http://gimp.org/>).

The HTML version of this manual was generated from DocBook XML using libxslt (<http://www.xmlsoft.org/XSLT/>) with customized XSLT stylesheets. More information about our documentation process is available at <http://www.e-smith.org/docs/> Most of the editing was done by Dan York and Kirrily "Skud" Robert using the vim (<http://www.vim.org/>) editor.

1.1.2. History

- **January 2002** - First print edition of the *SME Server V5.1 with ServiceLink User Guide* published by Mitel Networks Corporation Also published online in HTML and DocBook XML/SGML. Available at: <http://www.e-smith.org/docs/manual/5.1/> Primary author/editor Dan York.
- **August 2001** - First print edition of the *SME Server V5 with ServiceLink user's manual* published by Mitel Networks Corporation. Also published online in HTML and DocBook XML/SGML. Available at <http://www.e-smith.org/docs/manual/5.0/> Primary author/editor Dan York.
- **February 13, 2001** - *e-smith server and gateway user's manual* for version 4.1 published online in HTML and DocBook SGML by e-smith, inc. Available at <http://www.e-smith.org/docs/manual/4.1/> (<http://www.e-smith.org/docs/manual/4.1/>) Primary author/editor Dan York.
- **December 4, 2000** - *e-smith server and gateway user's manual* for version 4.0 published online in HTML and DocBook SGML by e-smith, inc. Available at <http://www.e-smith.org/docs/manual/4.0/> (<http://www.e-smith.org/docs/manual/4.0/>)
- **July 2000** - *e-smith server and gateway user's manual* for version 4.0 published in print form by e-smith, inc. PDF and PostScript versions also made available via FTP at <ftp://ftp.e-smith.net/pub/e-smith/e-smith-4.0/> (<ftp://ftp.e-smith.net/pub/e-smith/e-smith-4.0/>). Primary author/editor Ross Laver using StarOffice 5.1.
- **November 1999** - *e-smith server and gateway user's manual* for version 3.1 published in print form by e-smith, inc. Primary author Kim Morrison using StarOffice 5.1.

1.1.3. Endorsements

This is the official documentation for **SME Server V5 with ServiceLink** and is endorsed by Mitel Networks Corporation

1.1.4. Acknowledgements

Mitel Networks Corporation wishes to thank all of the developers in the open source community who continue to help us make our product better.

We also thank Craig Foster and Paul Miller for their help in documenting Macintosh connectivity.

1.2. Software Licensing Terms and Conditions

The SME Server V5 with ServiceLink is licensed for an individual server under the terms of the ServiceLink End User License Agreement found on the CD. Acceptance of this agreement is required during the software installation.

The SME Server V5 with ServiceLink kit also includes software that is distributed under the terms of the GNU General Public License or other open source licenses. SME Server V5 users may copy and redistribute this software. The text of the GPL license may be found on the web at <http://www.fsf.org/copyleft/gpl.html>. The applicable license for each software module is specifically identified and can be seen by running the **rpm -qiv packagename** command, from the command line, or is listed on our development web site at <http://www.e-smith.org/>

If you have acquired the March Networks SME Server V5 by means other than purchasing a Mitel Networks commercial offering through an authorized reseller, it is unsupported. For further information and available options, please contact an authorized reseller. A list of authorized resellers can be found at <http://www.mitel.com/sme/>.

1.3. About Our Test Company: The Pagan Vegan

In this user's guide, we use examples of a catering and event-planning company, The Pagan Vegan or TPV, that configures, administers and makes use of their server. As far as we know, no company of this name exists.

1.4. What's New

For the most complete list of information about changes that have been made in SME Server V5 with ServiceLink, see the release notes that accompany your software.

1.4.1. ServiceLink

- **Server file virus scanning** - The Virus Protection service can now be configured to scan all home directories and i-bays for viruses in addition to e-mail messages and attachments.

1.4.2. Server Features

- **User quotas** - Through a new web panel, you have the ability to set a limit on the amount of a disk space a user can use for files and e-mail.
- **USB printer support** - It is now possible to connect the SME Server to a printer via the USB port. The printer configuration panel has also changed slightly.
- **Improved Macintosh file sharing support**- The server now includes better support for Macintosh file sharing and eliminates some previous cases where Macintosh users were unable to access i-bays.
- **Experimental ISDN card support** - While our software has always supported external ISDN adapters, this version now includes experimental support for using an internal passive ISDN card.

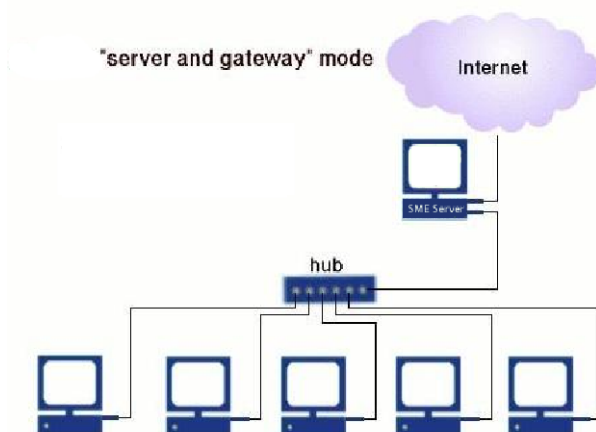
Chapter 2. The role of the SME Server V5

Your SME Server V5 with ServiceLink manages your connection to the Internet by routing Internet data packets to and from your network (which allows all the computers on your network to share a single Internet connection) and by providing security for your network, minimizing the risk of intrusions.

When one of your local computers contacts the Internet, or is contacted by an outside machine on the Internet, the SME Server V5 with ServiceLink not only routes that connection, but seamlessly interposes itself into the communication. This prevents a direct connection from being established between an external computer on the Internet and a computer on your local network thereby significantly reducing the risk of intrusion onto your network.

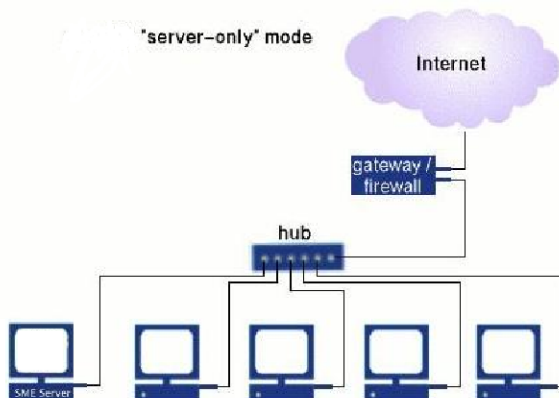
Your server also provides services - including e-mail, web access and a powerful file sharing and collaboration feature called "i-bays" - that allow you to communicate better internally and with the rest of the world using the Internet.

Throughout this user's guide, the word **gateway** is used to mean the computer that acts as the interface between your local, internal network and the external world.



If you prefer, you can also run your SME Server V5 with ServiceLink in "server-only" mode. In "server-only" mode, your server provides your network with services, but not the routing and security functions associated with the role of "gateway". The server-only mode is typically used for networks already behind a firewall. In that configuration, the firewall fulfills the role of gateway, providing routing and network security.

Once installed, your SME Server V5 with ServiceLink can be configured and managed remotely. Routine administration is handled from your desktop using a web-based interface, so only on rare occasions will you require direct access to the server computer. Once installation is complete, most customers put the server in an out-of-the-way place like a utility closet. If you wish, you can disconnect the keyboard and monitor. (Note that some computers may not operate correctly without an attached keyboard.)



More About Ethernets

Appendix A: Introduction to the Ethernet Local Area Network (LAN), briefly explains ethernet, ethernet components and typical ethernet configuration.

Chapter 3. ServiceLink

With SME Server V5 with ServiceLink, Mitel Networks Corporation has introduced a suite of integrated network services - *ServiceLink* - that extend and enhance the functionality of your server. ServiceLink maximizes the security, performance and reliability of your server through real-time interaction with the *Mitel Network Operations Center (NOC)*. You can register for ServiceLink by contacting any Mitel Networks Corporation authorized reseller and choosing a subscription plan that meets your needs. Note that until you register for ServiceLink, the links to ServiceLink pages in the server manager will take you to panels that are not active.

Note: If your server is behind an additional firewall, that firewall will need to be configured to allow *outbound* SSH packets on TCP port 22 in order for ServiceLink to function.

ServiceLink provides the following services:

- **24x7 Alerts and Reporting**

This service provides round-the-clock monitoring of your server and your Internet connection. By default, your server will synchronize with our NOC once each hour. (This can be customized by your Mitel authorized reseller.) If the server fails to check in, an alert is sent to your authorized reseller and, if desired, your network administrator.

In addition, Mitel Networks Corporation compiles monthly reports summarizing all ServiceLink activity for your authorized reseller who in turn can share the information with you. These reports include such details as network performance, e-mail delivery problems and viruses detected. Among other things, this information can help you and your authorized reseller assess the reliability and quality of your Internet connection. It can also assist in analyzing the security of your network.

- **Virus Protection**

This service provides automatic setup and configuration of e-mail and file virus-scanning services. Your server includes special virus-scanning software. When you subscribe to ServiceLink, your authorized reseller will activate this special software. Your server will then download the latest virus pattern files from the Mitel Networks NOC. All e-mail messages and attachments received from that point on will be scanned for viruses. In the event that a virus is found, the message will *not* be delivered. Instead, the sender, all intended recipients and your Mitel authorized reseller will be notified of the virus. The message itself will be quarantined in a special mailbox where the administrator can examine the message and determine what to do with it.

Through the server manager, you can also enable the nightly scanning of all home directories and i-bays for viruses. If infected files are found, the administrator will be notified by e-mail and can take the appropriate action.

Virus pattern files contain the information required to accurately identify viruses. As new viruses are detected, anti-virus software manufacturers update their pattern files. Your server's virus-scanning service automates the downloading and installation of new virus pattern files and ensures that the server is always capable of identifying the latest known threats.

Warning

The number of users for which virus protection can be provided is limited by the ServiceLink options you have chosen. If you configure your server for more than the supported number of users, virus protection will automatically be *disabled*. The service can, however, be upgraded to support a higher number of users. Please contact your authorized reseller for more information.

- **Guaranteed E-mail**

This service provides a backup e-mail service if a server becomes unreachable and cannot receive mail. The most common reason for this is a temporary failure of the Internet connection provided by your ISP. With ServiceLink, mail that cannot be delivered to your server will be stored at the NOC. Simultaneously, notifications are sent to your Mitel authorized reseller, who can investigate the cause of the outage.

This service uses what is called an *MX secondary*. Every domain name on the Internet has a record in the DNS which indicates which system should act as its primary mail exchanger ("MX" for short). When someone sends an e-mail, his or her local mail server will look for the recipient's MX and send the e-mail to it. If the MX is unreachable due to a system or network outage, the mail may be queued or it may bounce back to the sender.

The guaranteed e-mail service provided to ServiceLink subscribers works by configuring the DNS to use the NOC as a secondary MX. Therefore, if the primary MX is unreachable, the sender's mail server will send the e-mail to the secondary MX – in this case, the NOC. All e-mail collected in this fashion will be forwarded to your server as it becomes available again.

There is nothing that needs to be done to configure the guaranteed e-mail service. As soon as the NOC starts publishing your domain through the DNS service, the NOC will be set up to act as an MX secondary and start guaranteeing the delivery of your e-mail.

In addition to storing the e-mail and eventually forwarding it, the Mitel Networks NOC provides notification and reporting to your Mitel

- **DNS Services**

One of the components of a full Internet solution is a domain name. Most businesses using the SME Server V5 with ServiceLink will want to register a domain name representing their business, and will need a DNS host to make this domain name accessible to the world.

For reasons of security and reliability, the server is not configured to publish DNS records by itself. (Any network server can be configured to act as a public DNS server, but doing so can create a serious security vulnerability.) A properly administered DNS host needs to be stable and always on the Internet, which is why a Network Operations Center such as that of Mitel Networks Corporation is ideally suited to the task.

The domain name hosting service provided by ServiceLink allows you to publish domain name records via our NOC. In addition to any domain names you may have registered, you will also be able to use the special *e-smith.net* domain. This provides a low-cost alternative for small businesses or home users who do not wish to pay registration fees for a .com or other domain. Users may register their server with a name such as "mycompany.e-smith.net".

- **IPSEC VPNs**

As discussed in the section on remote access, your server provides support for *client-to-server* Virtual Private Networks (VPNs) using PPTP. ServiceLink provides the additional ability to create *server-to-server* VPNs using the highly secure IPSEC standard. This service allows you to link together servers in different physical locations to make one seamless "virtual" network. Information sent via this network is encrypted to prevent "snooping" by others on the Internet.

Note: The size of the VPN which can be supported may be limited by the ServiceLink options you have chosen. Contact your authorized reseller for more information.

To encrypt network traffic between servers, the server uses the *IPSEC protocol*. This system uses an encryption technique known as *public key cryptography*. In simple terms, each server connected in a VPN knows the *public key* of each of the other servers on the network; it uses that key to encrypt data intended for that server. A *private key* on the receiving server is then used to decrypt the data.

One of the difficulties in setting up a VPN is securely exchanging the keys required to set up the VPN. ServiceLink simplifies and automates this process via a trusted central exchange – the Mitel Networks NOC. In addition, ServiceLink also secures and automates the renewal of encryption keys.

When you establish a VPN using ServiceLink, one server is designated to act as the "primary" server - the server whose user accounts will be accessible via the VPN. The other servers in the VPN (known as secondary servers) will function as gateways for the users on their local networks.

Chapter 4. Your Internet Service Provider (ISP)

Your ISP is your connection to the Internet - it routes Internet data packets to and from your server. It also provides other essential services. This section of the user's guide reviews what ISPs offer and what the implications are in choosing among the various options available to you. While your ISP can also assist you in selecting and arranging the right Internet services for your organization, it's important to know the general range of services available, since not all ISPs offer all services.

Warning

If you are operating the product in "server-only" mode, you will need to review your gateway/firewall documentation and perhaps consult with your ISP regarding your configuration. For example, depending on your plans for the server, your ISP may need to publish DNS records associating your mail and/or web servers with your firewall IP address. You may also need to configure your firewall for port forwarding of services.

In server-only mode, the single Ethernet connection to the local network is "trusted" as being secure and packet filtering is disabled. For that reason, a server-only server must *always* be behind a local firewall. You should **not** directly connect such a system to the Internet via an Internet Service Provider.

4.1. Dedicated versus dialup connectivity

Connectivity, also referred to as Internet access type, refers to the physical connection between your site and your ISP. How you connect to your ISP affects the speed of your Internet connection, which, in turn, impacts such things as how quickly your web site is displayed to visitors.

Dedicated connectivity refers to a full-time connection to your ISP. Although they are more expensive than the alternative, dedicated connections are generally faster and allow you to use the full range of services on your server. There are several common types of dedicated connectivity. **ADSL** provides relatively fast data transmission over phone lines. A **cable connection** links you to your cable company, which provides you with many (though not all) of the same services as a traditional ISP. The speed of transmission over a cable network can vary widely (from quite fast to very slow) based in part on the usage within your neighborhood.

If you have **dialup** connectivity, your server is not permanently connected to the Internet. Rather, it connects to your ISP over a phone line using a **modem** or *ISDN adapter*. Because your connection to the Internet is not permanent, some of the services on your server cannot be provided to the outside world. For example, having your server host your external company web site would create a problem because whenever your server was not connected to the Internet, the web site would not be available. (However, it could certainly host an intranet web site because the local network would always be connected.)

4.2. The IP address

An IP address is an identifying number assigned to all devices connected to the Internet, and is used in routing information from one device to another. Like your phone number, your IP address enables other people to reach you. In our standard configuration, your ISP only needs to allocate one IP address for your network. It is assigned to your server, which will accept all the Internet data packets intended for your network and distribute them to the appropriate computer - much like an office receptionist is able to accept incoming calls and direct them to the appropriate extension.

4.2.1. Static versus dynamic IP addressing

A **static IP address** never changes. It is permanently assigned to your server by your ISP.

Note: Static IP addressing is preferable to dynamic IP addressing because it makes it easier for users on the Internet to connect to your services.

Dynamic IP address assignment means that your IP address is assigned to you only temporarily and may be changed by your ISP. This makes it more difficult to ensure continuity of service to your network. Consider again our telephone number analogy. When your telephone number changes, you are able to place outgoing calls. However, until your new phone number is registered with Directory Services, other people are unable to look up your new number and place calls to you. Similarly, whenever your IP address changes, a record associating your server with its new IP address must be published with the equivalent of Directory Services (known as Domain Name Service or DNS) before incoming traffic can find you.

If your IP address is dynamically assigned and you have a dedicated connection to your ISP (for example, with a typical cablemodem), you may find it helpful to use a **dynamic DNS service**. We strongly recommend you review Appendix B: Dynamic DNS services for more information about this worthwhile option.

Tip: ServiceLink subscribers will have all their DNS needs taken care of as part of the base package and can use either a static or dynamic address without having to use an additional dynamic DNS service.

4.2.2. Routable versus non-routable IP addresses

If an IP address is analogous to your phone number, then a **routable** IP address is the equivalent of a full telephone number complete with country code and area code such as +1-613-555-1234. Using the same analogy, a non-routable address is the equivalent of an office extension. If your server is assigned a **non-routable** address, it cannot directly receive incoming Internet connections, which limits the services that it can provide to your site.

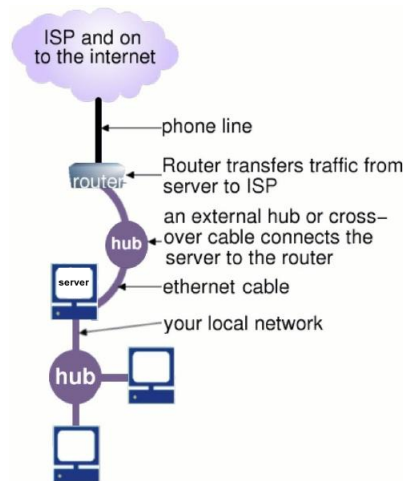
4.3. Arranging connectivity with your ISP

If you are going to be using your server in "server and gateway" mode, you will need to arrange for a connection to the Internet. Your ISP will help you connect your site and provide you with services that enable you to take advantage of the Internet (e.g. e-mail delivery). To some extent, the type of connection used determines the services needed. Therefore, we guide you first through arranging connectivity and then direct you to the appropriate list of services for each type of connection. The terms used in the following sections are defined at the end of this chapter.

To connect your site to the Internet, you not only need to arrange your physical connection (modem, ISDN, DSL, cable modem, etc.), but you also need to ensure that your server can locate the appropriate devices at your ISP's site. Your ISP will give you this information (e.g. IP addresses for their devices) which must eventually be entered into your server console (a straightforward process covered in a later chapter). Many ISPs use a DHCP server which can directly configure your server with some or all of these parameters.

4.3.1. Ordering a corporate ADSL or other commercial dedicated connection

Typically, your ISP will arrange for and configure your external hub and router. Alternatively, you may be required to install that hardware yourself under their direction. If a special phone line is required, the ISP will typically arrange that. It is most typical with corporate service that you receive a routable, static IP address. In fact, usually you will be allocated a block of routable, static IP addresses for your corporation - you will need only one for your server.



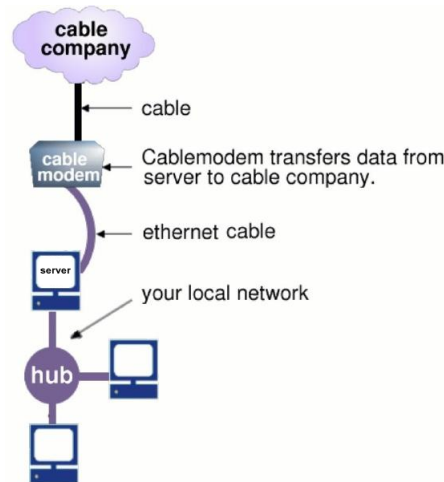
Information provided to you by your ISP:

- static IP address (or block of addresses from which you choose one)
- IP address of router ("gateway IP address")
- subnet mask

Order services from: Service List A

4.3.2. Ordering cablemodem or residential ADSL service

Typically, your cable company or ADSL provider will install a configured cablemodem or ADSL router at your site. If you do not have cable access, your cable company will install it for you. ADSL connects to the ISP via a conventional phone line. If you require an additional phone line, it is typical for you to arrange that yourself. There are three possible configurations when ordering cablemodem or residential ADSL services.



Note: In the tables below, please keep the following information in mind:

1. ISPs often supply the items marked * to your server by DHCP.
2. Some ISPs block outgoing HTTP connections, forcing you to use their proxy server. This interferes in a few minor ways with your server (e.g., the test for Internet connectivity will fail erroneously). However, using the ISP's proxy server will normally work fine.

1. You receive a routable, static IP address

Information provided to you by your ISP:

- static IP address
- IP address of cablemodem or ADSL router ("gateway IP address")
- subnet mask

Order services from: Service List A

2. You receive a routable, dynamically assigned IP address and you elect to use a dynamic DNS service (We encourage you to review *Appendix B: Dynamic DNS Services* for a discussion of dynamic DNS services.)

Information provided to you by your ISP:

- gateway IP address*
- subnet mask*

Information provided by dynamic DNS service:

- DNS service account name
- DNS service password

Order services from: Service List B

3. You receive a routable, dynamically assigned IP address and you elect not to use a dynamic DNS service OR your IP address is non-routable.

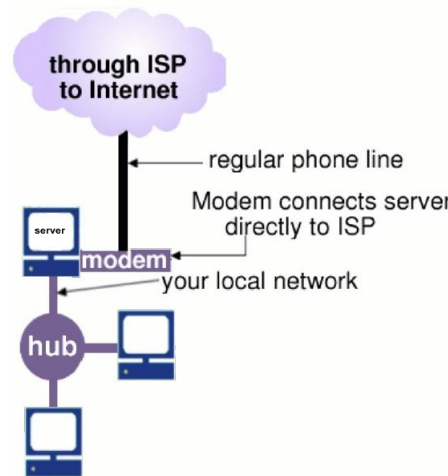
Information provided to you by your ISP:

- IP address of cablemodem or ADSL router ("gateway IP address")*
- subnet mask*

Order services from: Service List D

4.3.3. Ordering a dialup connection

It is typical for you to purchase and install your own modem or ISDN adapter for your dialup connection. (Be sure to use a Linux-compatible modem - WinModems will not work.) Your modem connects to your ISP over a conventional phone line. If you require an additional phone line, it is typical for you to arrange that yourself.



Your ISDN adapter will connect to the ISDN connection installed by your ISP or local telecommunications provider. The software can work with external ISDN adapters and includes support for passive ISDN cards.

Warning

While the software includes experimental support for ISDN cards, we do not provide technical support for the use of these cards as they have not yet been tested in a wide enough variety of environments.

There are two possible configurations with dialup service:

1. Your ISP is able to meet all of the following three conditions:

- you receive a routable, static IP address
- your ISP will provide a secondary mail server for your domain, which receives e-mail when your server is not connected.
- your ISP is able to accept the "ETRN command". (This command is used by the server to retrieve the mail held by the ISP's secondary mail server.)

Information provided to you by your ISP:

- static IP address
- dialup access number
- dialup account name
- dialup account password

Order services from: Service List C

2. Your ISP is unable to meet all three of the above conditions

Information provided to you by your ISP:

- dialup access number
- dialup account name
- dialup account password

Order services from: Service List D

4.4. Arranging Services From Your ISP

In each section on connectivity, above, we direct you to the appropriate list of services that should be ordered from your ISP.

4.4.1. Service List A

- domain name set up and hosting
- publication of DNS address records for your web server, FTP server and e-mail server
- publication of DNS mail (MX) records
- secondary mail server (optional)
- Internet news server (optional)

4.4.2. Service List B

Services to order from ISP:

- secondary mail server (optional)
- Internet news server (optional)

Services From Dynamic DNS Service

- domain name (depending on the service purchased, your dynamic DNS service may restrict what your domain name can be)
- publication of DNS address records for your web server, FTP server and e-mail server
- publication of DNS mail (MX) records

4.4.3. Service List C

- PPP dialup access (with static IP)
- domain name
- publication of DNS address records for your e-mail server*
- publication of DNS mail (MX) records
- secondary mail server (ETRN must be supported)
- Internet news server (optional)

Your web and FTP servers are available to the external world only when your server is connected to the Internet. DNS address records for web and FTP servers only need to be published if it is likely that someone external to your site will need to connect to them for a particular reason.

4.4.4. Service List D

Please read the important notes (below) on the limitations of this configuration.

- PPP dialup access (if you are using dialup connectivity)
- POP mailbox (with generous size limitation)
- domain name - route all mail for domain name to the single POP mailbox
- Internet news server (optional)

Some Important Notes on Service List D (Multidrop Mail)

Service list D is applied to configurations where the publication of DNS records is not practical either because your IP address changes frequently or because it is non-routable. Because there is no published address receiving incoming network connections, this configuration does not allow you to host a web page or FTP site using your SME Server V5 with ServiceLink.

In this case, e-mail is handled using a method called "**multidrop**", which involves temporarily storing all e-mail messages addressed to your domain in a POP mailbox at your ISP until your server connects and fetches them. Your POP mailbox must be large enough to hold the e-mail for your organization until it is fetched. If your primary ISP cannot supply this, you can use another ISP for your e-mail hosting.

As e-mail messages are delivered into the POP mailbox at your ISP, some of the addressee information is removed. To determine to whom the e-mail message is addressed, your server uses several heuristics. This works very well for normal person-to-person e-mail. However, messages from **mailing lists** (and other sources where the user's account name is not present in the headers) cannot be delivered. Any e-mail that cannot be delivered will be returned to the sender. If the e-mail cannot be returned to sender, it will be directed to the system administrator.

Some ISPs add a header to each e-mail message as it enters the POP mailbox to assist in determining the addressee. One common header tag is: "X-Delivered-To". If your ISP does this, make note of the header tag used so that you can configure your server to look for it (explained in a later section).

Because of the potential problems involved with delivery of e-mail to multidrop mailboxes, we strongly encourage you to consider other means of mail delivery before resorting to using multidrop.

Terms used in ordering connectivity and services**ADSL (or DSL)**

ADSL is a type of high-speed Internet access that uses regular phone lines and is available in many metropolitan areas.

Domain Name

This refers to the unique name attached to your organization on the Internet. For example, "tofu-dog.com" or "e-smith.com". If you don't have a domain name, your ISP can help you select one, ensure it is available, and register it.

DNS (Domain Name Service)

DNS, or Domain Name Service, refers to the software and protocols involved in translating domain names to IP addresses. Your server provides DNS lookup services for your local network, and your ISP typically also provides you with the IP addresses of DNS servers. These servers do **not** need to be configured into your server as the DNS server that is provided with your server will correctly resolve all local and Internet names.

DNS: Publication of DNS Address Records

The publication of DNS address information allows other DNS servers to look up your domain information. Your ISP must publish DNS address records associating the name of your web server ("www.domain.xxx"), FTP server ("ftp.domain.xxx") and e-mail server ("mail.domain.xxx") with the IP address of your server.

DNS: Publication of DNS Mail (MX) Records

The publication of DNS mail (MX) records is the method used to inform Domain Name Services worldwide that all e-mail to your domain ("yourdomain.xxx") should be delivered to your e-mail server ("mail.yourdomain.xxx").

ETRN

ETRN is a command used for dialup solutions in order to retrieve e-mail temporarily stored at your ISP

Gateway IP Address

A gateway is the device on your network that forwards packets to and from the Internet. The gateway IP address is the IP address for that device.

Internet News Service

If you want access to Internet newsgroups, your ISP will need to provide the IP address of an Internet news server. The ISP will provide direction in configuring your web browser or other newsreading software.

PPP

PPP refers to the "Point-to-Point Protocol" used when a modem connects to the ISP.

PPPoE

"PPP over Ethernet" is a modified version of PPP that is used over some high-speed ADSL connections to the ISP.

Secondary Mail Server

A secondary mail server receives e-mail for your domain if your server is unavailable, and reattempts delivery later.

Subnet Mask (or netmask)

A subnet mask (or a netmask) has four numeric segments (each between 0 and 255) and looks like an IP address. It enables your computers to deduce what network they are on. Your ISP provides the netmask for the external network between the ISP and your server.

Chapter 5. Hardware Requirements of the SME Server V5 with ServiceLink Host Computer

The hardware requirements of the SME Server V5 with ServiceLink are modest compared with other server software available today. However, because of its critical role in your office, selecting an appropriate host computer is important. The hardware requirements of the host computer depend on such things as the number of users on your network, whether you plan to use the proxy server on the server, and the speed of your Internet connection.

Because the SME Server V5 with ServiceLink software relies upon your computer meeting the hardware standards noted in this section, Mitel Networks Corporation cannot support a server installed on hardware that does not meet these standards.

Before you consider the requirements defined below, please be aware of the following notes:

- The server ships with the remote access services disabled by default. Enabling webmail will increase the resource requirements of your server, in particular the memory requirement. Other remote access services, such as ssh and PPTP, are also processor-intensive. You should consider a fast processor speed if you intend to make significant use of these services.
- The server should work with any Pentium, Celeron, AMD or Cyrix processor that can run Red Hat Linux 7.1.
- For a dedicated connection in server and gateway mode, your server requires two ethernet adapters (also called network adapters or network interface cards). For a dialup connection or server-only mode, one ethernet adapter is needed.
- SCSI (Small Computer Systems Interface) is a system for adding peripherals to a computer which enhances performance, reliability and scalability. If you are using a SCSI system, you will need a specific adapter/driver (installed similarly to an ethernet adapter) and will need to purchase SCSI-enabled peripherals. These tend to be more expensive than their non-SCSI counterparts but the tradeoff is often worth it if the system will be under heavy loads.

Note: Our hardware recommendations only apply to servers with up to 500 users. This is not a technical limitation, and the SME Server V5 with ServiceLink can provide services to more than 500 users. In that case, we suggest that you specify a custom system using our Category 4 requirements as the minimum starting point.

5.1. Hardware Requirements for a Category 1 Server

The following information outlines what we consider the minimum system that can give satisfactory performance as a basic file/print server and network gateway. Note that we do not believe such a system will provide satisfactory performance for features such as webmail, remote access via PPTP and for ServiceLink offerings such as automatic virus protection and IPSEC VPNs.

Table 5-1. Definition of a Category 1 Server

# of Users	Up to 10
Usage	Light (minimal use of remote access, file sharing and other disk-intensive activity. No use of webmail, virus scanning or VPNs.)

Table 5-2. Hardware Requirements for a Category 1 Server

Architecture	PCI-based Pentium-class processor
Processor speed	90 MHz (or better)
Minimum RAM	32 MB (64 MB recommended)
Hard drive	IDE or SCSI - at least 1 GB
SCSI adapter	SCSI adapter must appear on the supported list (only necessary for SCSI systems)
Ethernet adapters	The ethernet adapters installed on your server must appear on the supported list.
Modem (for dialup only)	Only modems that are Linux-compatible may be used. WinModems are not supported.
CD-ROM drive	ATAPI or SCSI
Floppy drive	any
Monitor	any
Graphics card	any
Mouse	none required

Sound card	none required
------------	---------------

5.2. Hardware Requirements for a Category 2 Server

Table 5-3. Definition of a Category 2 Server

# of Users	Up to 40
Usage	Light (moderate use of remote access, file sharing and other disk-intensive activity)

Table 5-4. Hardware Requirements for a Category 2 Server

Architecture	PCI-based Pentium-class processor
Processor speed	400 MHz (or better)
Minimum RAM	128 MB
Hard drive	IDE or SCSI - at least 6 GB
SCSI adapter	SCSI adapter must appear on the supported list (only necessary for SCSI systems)
Ethernet adapters	The ethernet adapters installed on your server must appear on the supported list.
Modem (for dialup only)	Only modems that are Linux-compatible may be used. WinModems are not supported.
CD-ROM drive	ATAPI or SCSI
Floppy drive	any
Monitor	any
Graphics card	any
Mouse	none required
Sound card	none required

5.3. Hardware Requirements for a Category 3 Server

Table 5-5. Definition of a Category 3 Server

# of Users	Up to 40
Usage	Heavy (heavy use of remote access, file sharing and other disk-intensive activity)

Table 5-6. Hardware Requirements of a Category 3 Server

Architecture	PCI-based Pentium-class processor
Processor speed	600 MHz (or better)
Minimum RAM	256 MB
Hard drive	IDE or SCSI (SCSI <i>highly</i> recommended) - at least 10 GB
SCSI adapter	SCSI adapter must appear on the supported list (only necessary for SCSI systems)
Ethernet adapters	The ethernet adapters installed on your server must appear on the supported list.
Modem (for dialup only)	Only modems that are Linux-compatible may be used. WinModems are not supported.
CD-ROM drive	ATAPI or SCSI
Floppy drive	any
Graphics card	any

Mouse	none required
Sound card	none required

5.4. Hardware Requirements for a Category 4 Server

Table 5-7. Definition of a Category 4 Server

# of Users	Up to 500
Usage	Heavy

Table 5-8. Hardware Requirements of a Category 4 Server

Architecture	PCI-based Pentium-class processor
Processor speed	700 MHz (or better)
Minimum RAM	256 MB
Hard drive	SCSI - at least 20 GB (2 large SCSI drives using RAID1 <i>strongly</i> recommended)
SCSI adapter	SCSI adapter must appear on the supported list
Ethernet adapters	The ethernet adapters installed on your server must appear on the supported list.
Modem (for dialup only)	Only modems that are Linux-compatible may be used. WinModems are not supported.
CD-ROM drive	ATAPI or SCSI
Floppy drive	any
Monitor	any
Graphics card	any
Mouse	none required
Sound card	none required

5.5. Supported Ethernet Adapters

Either one ethernet adapter (in the case of dialup connectivity or server-only mode) or two ethernet adapters (for dedicated connections in server and gateway mode) must be installed on your SME Server V5 with ServiceLink. This section describes which types of ethernet adapter can be used in the computer that will become your server. (There are no restrictions on the ethernet adapters in your other computers.)

Any adapters installed on the server must appear on the following supported list. Note that only PCI adapters are supported. The PCMCIA adapters used in many laptops and the older ISA adapters are not supported.

Note: Because SME Server V5 with ServiceLink is based on Red Hat Linux version 7.1, PCI ethernet adapters that can work with Red Hat 7.1 should also work with SME Server V5 with ServiceLink. You can find an up-to-date searchable database at Red Hat's web site at: <http://hardware.redhat.com/redhatready/cgi-bin/us/db-hcl.cgi> (Choose **Network Device/Controller** from the "Hardware Category" menu.)

If you need more information about how to install an Ethernet adapter, please visit our HOWTO document on "Installing an Ethernet Adapter in 11 Steps" found online at <http://www.e-smith.org/docs/howto/nicinstall-howto.html>

Be aware that your Mitel authorized reseller may not be able to support you if choose to use an adapter that is not on our supported hardware list. Please consult your Mitel authorized reseller for more information.

5.5.1. Supported Ethernet Adapters

The following PCI Ethernet adapters are supported by SME Server V5 with ServiceLink:

- 3Com 3C501, 3C503, 3C556, 3C590, 3C592, 3C595, 3C597

- 3Com 3C900, 3C900B, 3C905, 3C905B, 3C905C, 3C980, 3C985
- 3Com Megahertz 3CXE589D, EC, ET
- Accton EN1203, EN1207, EN1207(B,C,D,F), EN2212 EtherDuo PCI, SOHO BASIC EN220
- Adaptec ANA6901/C, ANA6911/TX, ANA6911A/TX
- ALFA GFC2206
- AMD
- Allied Telesyn AT-2550, AT-2560
- AMD 79c970 (PCnet LANCE), 79c978 (HomePNA)
- AT&T GIS (NCR) 100VG
- C-NET CNE-935
- Cogent EM100, EM110, EM400, EM960, EM964 (Quartet)
- Compaq NetFlex 3/P, Integrated NetFlex 3/P
- Compaq Netelligent 10 T PCI UTP, 10 T/2 PCI UTP/Coax, 10/100 TX Embedded, 10/100 TX PCI UTP, 10/100 TX UTP, Dual 10/100 TX PCI UTP, Integrated 10/100 TX UTP, ProLiant Integrated 10/100
- Compex ReadyLink 100TX, 2000, ENET100-VG4
- D-Link DE-530CT, DFE500-Tx, DFE540-Tx
- Danpex EN-9400P3
- DEC 21040, 21041
- Davicom Ethernet 100/10
- Farallon PN9000SX
- Fujitsu FMV-181, FMV-182, FMV-183, FMV-184
- General Instruments SB1000
- Genius GF100TXR (RTL8139)
- HP J2585A, J2585B, J2970, J2973
- IBM EtherJet PCI 10/100 adapter (i82557)
- Intel 82556, 82557, 82865
- Intel PCI EtherExpress Pro 10+, Pro100+, Pro100B
- Kingston EtherX KNE100TX, KNE110TX, KNE120TX, KNE20T, KNE30T, KNT40T, KNECB4TX
- Lite-ON LNE100TX
- Lucent WaveLan
- Macronix MX98713, MX987x5
- Microdyne/Eagle NE10/100 (i82557 w/DP83840 transceiver)
- NDC Communications NE100TX-E
- Netgear FA310TX 10/100, FA310TXC 10/100, GA620
- Novell NE1000, NE2000, NE2100, NE2500, NE3210, NL-10000
- Olicom OC-2183, OC-2325, OC-2326
- Racal Interlan ES3210
- Realtek 8029
- Samsung Smartether100 SC1100
- Sis 900
- SMC 8432T, 8432BT, EtherPower, EtherPower10/100, EZ 1208T, EZ 1211TX, 83C170QF, LANEPIC
- Surecom EP-320X
- Symbios 83C885, Yellowfin G-NIC
- Syskonnect Gigabit Ethernet
- Thomas Conrad TC5048

- Znyx ZX312 (EtherArray), ZX314, ZX315, ZX342, ZX344, ZX345, ZX346, ZX348, ZX351

If your adapter is not listed above, it may be supported if it is based on one of the following chipsets (check with Red Hat's web site mentioned above for confirmation):

- Alteon AceNIC Gigabit Ethernet
- Compex RL2000
- DEC Tulip
- KTI ET32P2
- NetVin NV5000SC
- RealTek RTL8029, RTL8029AS, RTL8129/8139
- VIA Rhine, VT86C926 "Amazon"
- Winbond 89C940

5.6. Supported SCSI Adapters

If the computer you plan to use for your server has a SCSI hard disk, your SCSI adapter must be supported by Red Hat Linux 7.1. PLEASE NOTE: Only PCI SCSI adapters are supported by the SME Server V5 with ServiceLink. Furthermore, they must contain a SCSI BIOS so that the PC can boot from the SCSI disk.

Note: As SME Server V5 with ServiceLink is based on Red Hat Linux version 7.1, PCI-based SCSI adapter that can work with Red Hat Linux 7.1 should also work with SME Server V5 with ServiceLink. You can find an up-to-date searchable database at Red Hat's web site at: <http://hardware.redhat.com/redhatready/cgi-bin/us/db-hcl.cgi> (*Choose **Storage Device/Controller** from the "Hardware Category" menu.*)

Because there are a very large number of SCSI adapters supported, the list below contains the overall categories of supported adapters. If your adapter falls into one of these categories, it is probably supported. Please check with your Mitel authorized reseller to verify support for your card.

Be aware that your Mitel authorized reseller may not be able to support you if choose to use a SCSI adapter that is not on our supported hardware list. Please consult your Mitel authorized reseller for more information.

Note: In the list below the use of an 'x' symbolizes a wildcard. For example, 'AHA-29xx' indicates it applies for the 'AHA-2930' as well as the 'AHA-2940' and any other models beginning with 'AHA-29'.

- Adaptec AIC-78xx, AHA-29xx, AHA-394x, 29160/39160, AHA-1520B
- Advansys ABP510, ABP514x, ABP930/40, ASC1200
- AMI MegaRAID
- Artop Electronic Corp AEC671x
- Dell PowerEdge RAID Controller 2¹, Expandable RAID Controller 2/3
- Future Domain TMC-18C30
- HP NetRAID-4M
- IBM ServeRAID
- ICP Raid Controller GDT 6xxx, GDT 7xxx
- Initio Corp INI-940, INI-950, INI-9100/9100W, 360P
- Intel 80960RP
- LSI MegaRAID express500
- Mylex (BusLogic) FlashPoint Series, MultMaster 01/10
- Symbios 53c1510, 53c8xx

1. Note that the firmware on this controller may need to be updated before it can work your server. See <http://www.e-smith.com/faq/> for more information.

- Q Logic QLA10160, 1080, 1240, 1280, 2100, 2200 12160

5.7. Supported Tape Drives

If you intend to use the tape backup capabilities of the SME Server V5 with ServiceLink, you must have a tape drive that will work with a Linux system.

We believe that most SCSI tape drives and many IDE tape drives will work correctly. Unfortunately, the popular *OnStream* tape drives do not at the current time work with Red Hat Linux version 7.1, and hence are not supported by your SME Server V5 with ServiceLink.

We have tested the following tape drives and know that they work with the SME Server V5 with ServiceLink:

Table 5-9. Supported SCSI Tape Drives

Vendor	Model	Revision	Format
Dell	Powervault 100T		DAT
HP	HP35470A	T603	DAT
Seagate	Python 06408	XXX	DAT
SONY	SDX-300C	0400	AIT

Table 5-10. Supported ATA (IDE) Tape Drives

Vendor	Model	Revision	Format
Seagate	STT20000A	8A51	
Seagate	STT32000A		

We have tested and verified that the following tape drives do *not* work with the SME Server V5 with ServiceLink:

Table 5-11. Unsupported ATA (IDE) Tape Drives

Vendor	Model	Revision	Format
OnStream	DI-30		ADR

If you do not have one of the supported drives listed above you may want to check with <http://hardware.redhat.com/> for information about how well that drive will work with Red Hat Linux 7.1.

Note: If your tape drive is not listed at Red Hat's site, you can visit <http://www.linuxtapecert.org/> to see if your tape drive vendor is participating with that tape drive certification effort. Be aware that some of the solutions developed to get certain tape drives to work with Linux may require kernel modifications and only be attempted by experienced developers. Please consult your Mitel authorized reseller for more information.

Chapter 6. Installing And Configuring Your SME Server V5 with ServiceLink Software

6.1. Licensing Terms and Conditions

In installing the SME Server V5 with ServiceLink software, you are agreeing to the open source licensing terms and conditions associated with it. You can read these terms and conditions in the introduction to this guide under the title *Software Licensing Terms and Conditions*.

Warning

The computer on which you install this software will be totally dedicated to being your SME Server V5 with ServiceLink. The hard drive of this computer will be erased and re-written with the Linux operating system - dramatically enhancing the reliability of your server over other operating systems. However, this means that while this computer is acting as your server, you cannot use it for any other purpose.

Note: If you have previously installed and configured a server and are reinstalling the software, please be aware that you must use the Upgrade option in order to preserve your existing configuration and data. Simply performing a new installation will erase all previously existing user accounts, user directories, i-bay contents and web site and configuration parameters. If you have not already done so, you may wish to back up the contents of your server onto one of your desktop computers. You can do so easily by selecting "Backup or restore" from the server manager, as explained in the chapter on on-going administration of your server.

6.2. RAID1 Support (Disk Mirroring)

With SME Server V5 with ServiceLink, you have the ability to set up disk mirroring, also called RAID Level 1. In disk mirroring, you basically write all of your data to two separate hard disks installed in your server. One is the mirror of the other. Should the primary disk experience a hardware failure, the mirror disk will continue operations as if nothing had happened. All of your data will be protected.

Disk mirroring can be accomplished through either *software* or *hardware*.

6.2.1. Software Mirroring

To enable software RAID1 support, you must first have two disks that are either the same size or capable of having partitions of the same size. They can be either SCSI or IDE drives. **They must both be installed in your system prior to installing the SME Server V5 with ServiceLink software. Software RAID support can *only* be configured at the time you install the software.** If you choose not to configure RAID support on your server, and later wish to do so, you will need to reinstall the SME Server V5 with ServiceLink software.

Once you have two disk drives, activating RAID support requires only a very slight change in the software installation process.

Note: SME Server V5 with ServiceLink supports a software implementation of RAID Level 1, known as disk mirroring. It does *not* support RAID Level 0 (disk striping), as that does not provide any protection of your data whatsoever. It does not support RAID Level 5 (disk striping with parity) because of the poor performance and reliability of software implementations of RAID5. If you are seeking RAID5 support, Mitel Networks Corporation recommends you consider one of the many hardware implementations which will provide both protection and performance.

6.2.2. Hardware Mirroring

With hardware mirroring, you use a special RAID disk controller to perform the actual mirroring across multiple disks. As mirroring is performed in hardware, the performance can be significantly faster than software mirroring. Additionally it can simplify configuration because to the operating system the entire RAID disk system looks like one single disk. You should be able to use any supported SCSI hardware RAID controller.

If you are going to use hardware mirroring, you should **NOT** choose *Install - Dual hard disk with software RAID-1 mirroring* in the installation process. (Doing so will enable *software* mirroring.) Instead, you should do a regular installation of the software.

Note: Using one of the supported hardware RAID controllers, you *will* be able to upgrade from an earlier version of the SME Server to version 5.1 using the standard upgrade process. You should back up all your data and test carefully after installation.

6.3. Upgrading From A Previous Version

If you have previously installed a server and now wish to upgrade to version 5.1, you *can* do so while preserving your configuration data. To do so, select **Upgrade** from the appropriate screen in the installation process.

While the upgrade should proceed smoothly, we do recommend that you back up your system prior to performing this upgrade just to be safe.

Warning

It is not possible to use the **Upgrade** option to *add* software mirroring (RAID1) to an existing server.

If you previously installed software mirroring with a previous version of the software, you should be able to upgrade without any problems. However, if you want to upgrade a previous version of the software that was *not* installed with software mirroring to use software mirroring (RAID1) support, you should:

1. perform a backup through the server manager
2. perform a fresh install selecting the software mirroring option
3. restore the backup through the server manager

6.4. Installing the Software

Note: If you are configuring your system with RAID1 support, notice that your step 4 below will be slightly different. If you skipped the previous section on RAID, it would be advisable to read it before proceeding.

Step 1: Insert the CD-ROM. If your computer is an older model that is unable to boot from CD-ROM, you will also need to insert the boot floppy. Most modern computers do not need to use a boot floppy.

Step 2: Review the warning screen and type **accept** to indicate your acceptance of Mitel Networks Corporation's legal terms and conditions and your acknowledgment that installation of the software will rewrite the host computer's hard drive.

Warning

The installation process formats and erases **all attached hard drives**. If you have multiple hard drives, be sure to back them up prior to starting the installation process.

Step 3: Read the software licensing terms and indicate your acceptance of the license.

Step 4: Choose whether you wish to *Install on a single hard disk (or use hardware mirroring)*, *Install on dual hard disks using software mirroring* (RAID1 support), or *Upgrade*.

Step 5: Read the screen offering a final warning. Type **proceed** and hit enter on the "OK" button to continue. The installation process will now automatically proceed to install the necessary packages.

Step 6: Indicate whether you wish to create an emergency boot diskette. This can be used in the future to boot the system in the event that you are unable to boot from the hard disk. If you choose yes, you will be prompted to insert a blank diskette. We recommend that you *do* create an emergency boot floppy and put it in a safe place where you can easily retrieve it when necessary.

Step 7: Finishing the installation is automatic and takes only a few minutes. At the end of the process, you will be prompted to remove the floppy diskette and CD and then to reboot your computer.

Warning

The installation (or upgrade) process rewrites the boot sector on your hard drive. This may cause machines with BIOS boot sector virus detection to not boot unattended. This detection should be disabled in your system's BIOS.

6.5. Configuring your SME Server V5 with ServiceLink

Once your system has restarted (so that it is no longer booting from the installation CD), you are ready to configure your system.

If your ISP provided you with a summary of your configuration choices and network information, we suggest that you keep it handy while completing the screens in the configuration section of the server console.

There are several types of configuration parameters that must be entered into your server:

- the system password
- the type of ethernet adapters (network interface cards, or NICs) that will be used by your server to communicate with the internal network and the Internet (or external network). Typically, the server software will detect this information automatically. (Note that if you are connecting to the Internet with a dialup connection, you only need one ethernet adapter.)
- configuration for the internal (local) network - you must provide information about your internal network so that your server can communicate with other machines on your local network.
- operation mode - you must select whether your server will operate in server and gateway mode or server-only mode.
- configuration for the external network/Internet - you must configure your server so that it can communicate with your ISP either by a dedicated connection or using a dialup connection (*only for server and gateway mode*).
- miscellaneous information - there are several final items to configure, such as whether to allow your users to use a proxy server, whether to provide status reporting to Mitel Networks Corporation, and whether you wish to secure the server console so that it can only be accessed using the administrator's password.

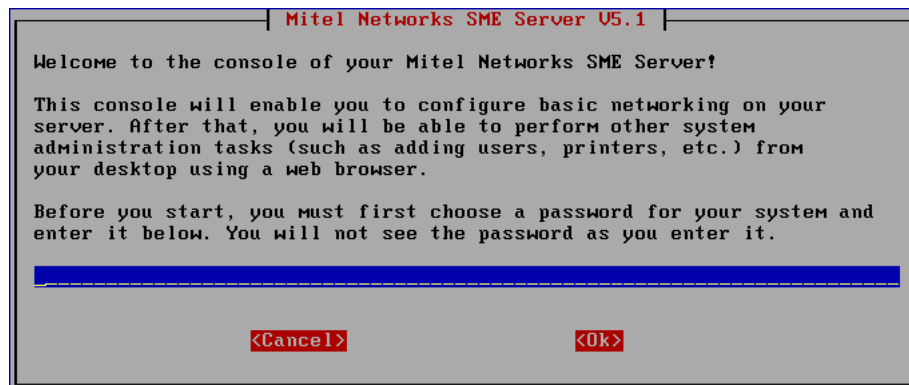
As you select a given configuration parameter, you will be presented only with the screens necessary for your given configuration. Each screen will provide you with a simple, detailed explanation of the required information.

Note: The "Keep" option: As you move through the configuration screens, you will notice that there is a "Keep" option which will allow you to keep the choices you may have made previously. Obviously, when you are configuring your system for the first time, many of these choices will not have been made, but if you later go back to re-configure the system, this option can save time.

6.6. Setting Your Administrator Password

As shown in the image below, the first thing you will be asked to do is to set the system password. This is the password you will enter to access the web-based server manager. Depending on how you configure the system, you may also need to enter this password to access the server console. It is *extremely* important that you choose a good password and keep that password secret.

Anyone who gains access to this password has the power to make *any* change to your server!

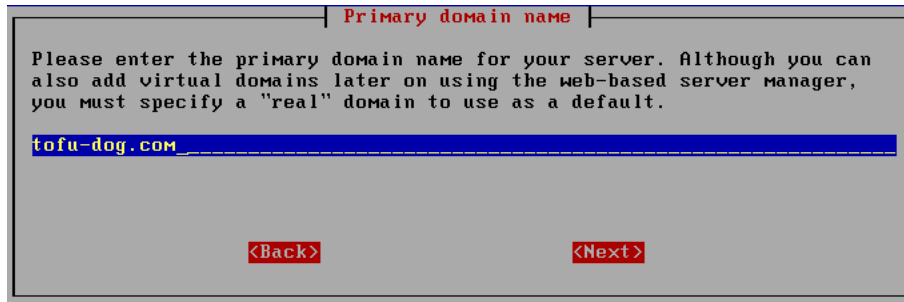


After you enter the password once, you will be asked to type it again to confirm that the password was recorded correctly. The password will also be examined to determine how strong it is from a security point-of-view. If it is found to be weak (for instance, a dictionary word), you will see an additional screen asking if you *really* want to use this password. You will have the option to go back and change to a stronger password or to continue using the weaker password.

Note: You can use any ASCII printable characters in the administrator password. As this password gives someone total control over your server, you should choose a password that cannot be guessed easily. A good password should contain mixed upper- and lower-case letters, numbers and punctuation, yet also be easy to remember. An example might be "IwmSMES!" as in "I want my SME Server!" (Please don't use this example as your password!)

6.7. Configuring Your System Name and Domain Name

As shown below, your next step is to enter the *primary* domain name that will be associated with your SME Server V5 with ServiceLink. (You can later configure other *virtual* domains that work with the server.)



Primary domain name

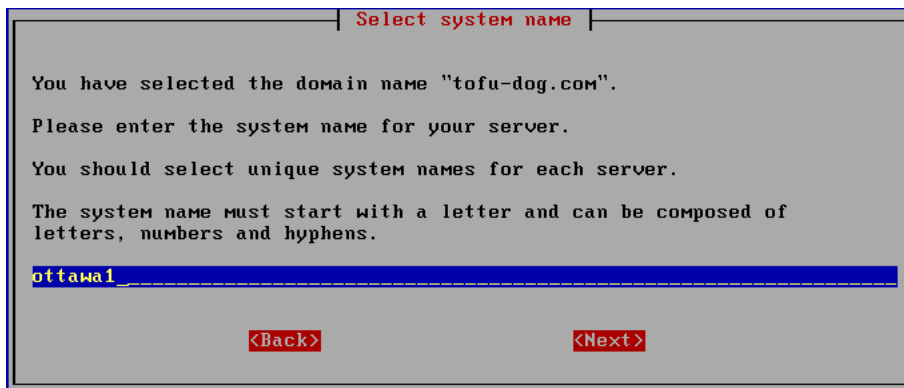
Please enter the primary domain name for your server. Although you can also add virtual domains later on using the web-based server manager, you must specify a "real" domain to use as a default.

tofu-dog.com

<Back> <Next>

Next you need to provide a name for your server. You should think carefully about this as changing it later may create additional work. (For instance, Windows client computers may be mapping drives to your server using its name. Those clients would need to remap the drive using the new name.)

Tip: You should make the system name as unique as possible in case you someday decide to link your server to another server using an IPSEC VPN. When you do, each server will need a unique name. Using some type of theme, such as location names, may be an effective way to ensure unique names.



Select system name

You have selected the domain name "tofu-dog.com".

Please enter the system name for your server.

You should select unique system names for each server.

The system name must start with a letter and can be composed of letters, numbers and hyphens.

ottawa1

<Back> <Next>

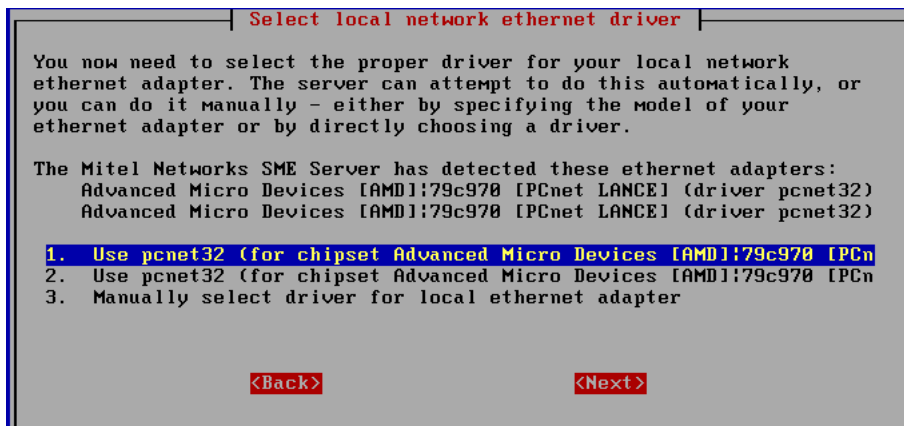
6.8. Configuring Your Local Network

6.8.1. Selecting Your Local Ethernet Adapter

An ethernet adapter - also called an ethernet card or network interface card (NIC) - is a special piece of hardware that serves as the interface between a computer and the ethernet network. It connects your computer and the ethernet, allowing the computer to communicate with other computers and devices on the network.

A computer needs a special software program, called an "ethernet driver", to use an ethernet adapter. Which ethernet driver is required depends on which ethernet adapter is installed on your computer.

You will first need to select the appropriate driver for the ethernet adapter connected to your local network, as shown in the screen below:



Select local network ethernet driver

You now need to select the proper driver for your local network ethernet adapter. The server can attempt to do this automatically, or you can do it manually - either by specifying the model of your ethernet adapter or by directly choosing a driver.

The Mitel Networks SME Server has detected these ethernet adapters:
Advanced Micro Devices [AMD]:79c970 [PCnet LANCE] (driver pcnet32)
Advanced Micro Devices [AMD]:79c970 [PCnet LANCE] (driver pcnet32)

1. Use pcnet32 (for chipset Advanced Micro Devices [AMD]:79c970 [PCn
2. Use pcnet32 (for chipset Advanced Micro Devices [AMD]:79c970 [PCn
3. Manually select driver for local ethernet adapter

<Back> <Next>

If you are using a PCI ethernet adapter that appears on our supported list, it is likely that your server will be able to detect your hardware automatically and you will simply be able to choose option 1, "Use xxxx (for chipset yyyy)", where 'xxxx' and 'yyyy' are specific to your hardware. If the software fails to detect it correctly, you can manually select the appropriate driver for your ethernet adapter from a list of drivers or from a list of ethernet adapter models. After the appropriate driver is selected, select "OK" and proceed to the next screen.

6.8.2. Configuring Local Network Parameters

Your SME Server V5 with ServiceLink needs information about your local network in order to communicate with the other computers on your network. This includes the IP address and the subnet mask on your server's internal interface. Because your server acts as a gateway and firewall, these will differ from the IP address and subnet mask on the external interface.

If you plan to operate in server and gateway mode (explained in greater detail below), your server will act as a relay between your local network and the Internet. Because no computer on your local network, other than your server, directly interacts with the external world, the IP addresses assigned to those computers need only be unique with regards to your local network. (It doesn't matter if a computer on someone else's local network uses the same IP address, because the two machines will not be in direct contact.) As a result, we are able to use special "non-routable IP addresses" for your local network, including the internal interface of your server.

Local networking parameters

Please enter the local IP address you would like to use for this server.

If this server is the first machine on your network, we recommend accepting the default value unless you have a specific reason to choose something else. If your server is being installed into an existing network, you must choose an address which is not in use by any other computer on this network.

192.168.202.1

<Back> <Next>

If you have no reason to prefer one set of IP addresses over another for your local network, your server will prompt you with default parameters that are probably appropriate in your situation.

Tip: If you are installing servers at multiple sites within your organization, you may find it useful for later troubleshooting to use different network addresses for each site. Additionally, if you ever want to establish an IPSEC VPN between the servers, each server will need to use a different range of IP addresses. Even if you are not planning to use a VPN right now, it would be safest to use unique network addresses for each location.

If, however, you are operating your server in "server-only" mode and there are already servers on your network, you will need to obtain an unused IP address for your local network.

Next, you will be prompted to enter the subnet mask for your local network. If you are adding your server to an existing network, you will need to use the subnet mask used by the local network. Otherwise, unless you have a specific need for some other setting, you can accept the default setting.

6.9. Operation Mode

After configuring your SME Server V5 with ServiceLink for your local network, you will see the following screen. This is where you select your server's operation mode.

Select operation mode

If you want this server to act as a gateway to the Internet, choose one of the server and gateway options. The private server and gateway mode disables all incoming services.

Server-only mode provides services to a local, protected network. If you choose this mode and Internet access is required, the network must be protected by another Mitel Networks SME Server configured in server and gateway mode (or another firewall).

keep Keep the current setting: "Server and gateway".

1. Server and gateway
2. Private server and gateway
3. Server-only

<Back> <Next>

6.9.1. Option 1: Server and gateway mode

In server and gateway mode, your server provides services (such as e-mail, web services, file and print sharing) to your network and also acts as a

network, and provides security and routing.

If you configure your server to operate in server and gateway mode, your server will require either:

1. two ethernet adapters (one to communicate with the local network and the other to communicate with the external network/Internet)
2. one ethernet adapter (for the local network) and a modem for a dialup connection

With server and gateway mode, there are a number of extra parameters that will need to be configured. These will be discussed in the next section.

6.9.2. Option 2: Private server and gateway

This mode is a variation of option 1 and provides the same functionality with the following differences:

- Your web server is not visible to anyone outside of the local network.
- Your mail server is not accessible from outside of the local network.
- Additional firewall rules have been configured to drop packets for various services (such as 'ping' requests).

All services *are* available on the internal network. The differences are entirely in how your server is seen by the external world.

You would select this mode only if you wish to use the server as a gateway, but do not wish to publish any services to the external Internet.

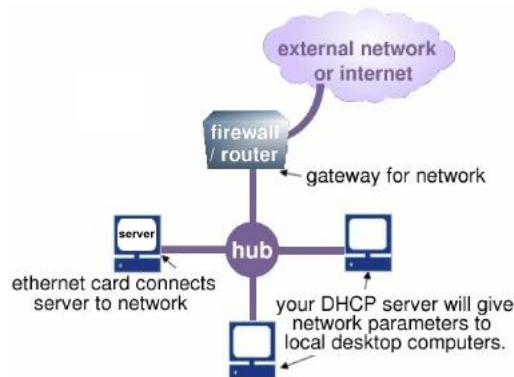
6.9.3. Option 3: Server-only mode

Server-only mode is appropriate if you do not wish to use the gateway capabilities of your server. In this configuration, your server connects only to the local network and does not connect directly to the outside world (although it may connect indirectly through your firewall or another server).

Warning

Because the server "trusts" the local network to be secure in server-only mode, it **must** be behind a firewall of some type. Under no conditions should it be directly connected to the Internet.

Your network will resemble the image below:

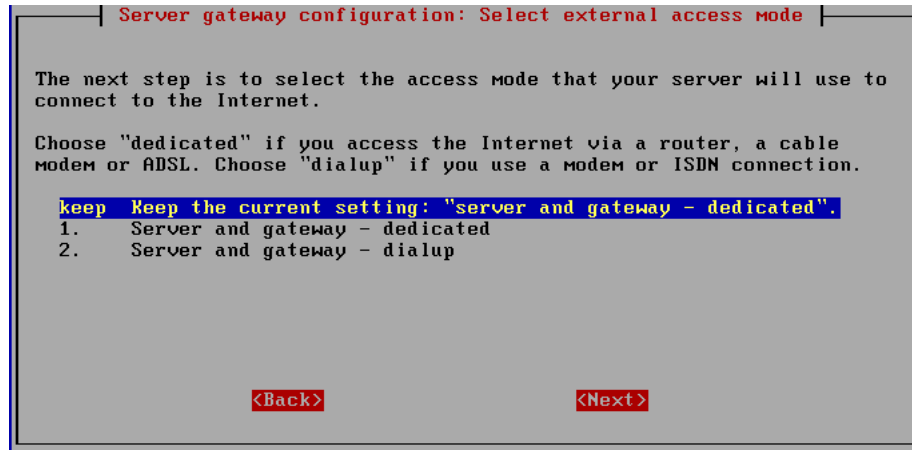


If you have a connection to the Internet by way of another gateway or corporate firewall, you can configure your server to provide services (including e-mail, web services, file and print-sharing) to your network. In this instance, you do not need your server to provide the gateway role because that role is fulfilled by your firewall. If you select Option 3, "**Server-only mode - protected network**", your server will provide your local network with web, e-mail, file and print-sharing.

On the next configuration screen, you should enter the IP address for the Internet gateway on your local network. If you do not have an Internet connection, simply leave this configuration screen blank.

6.10. Configuring Server and Gateway Mode

If you are configuring your server to operate in server and gateway mode, you must select one of two Internet connection types - a **dedicated connection** (such as ADSL or cable modem) or a **dialup connection** (in which case you will be connecting to your ISP via a modem).



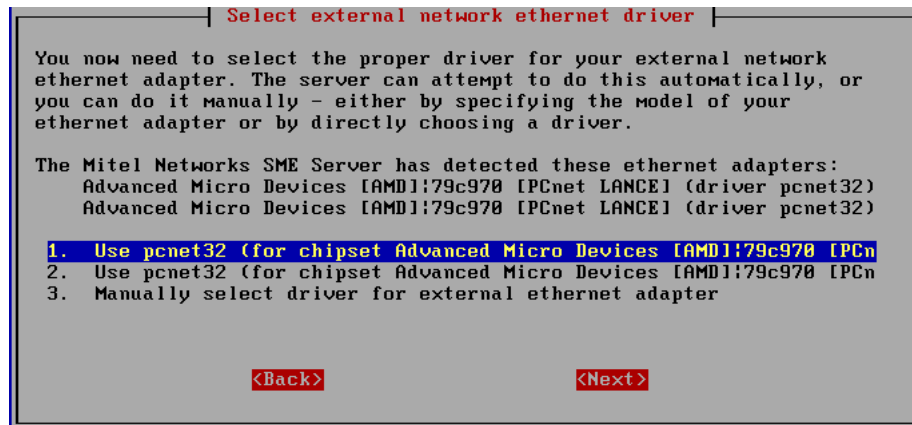
The next step after selecting a connection type is to enter the specific parameters representing that connection.

6.11. Server and Gateway Mode - Dedicated

How you configure your server's external interface depends on whether you are using a dedicated connection or a dialup connection. Therefore, if you configured your server for "server and gateway mode - dedicated connection" you will be presented with very different configuration screens than if you configured the server for "server and gateway - dialup connection" (as discussed in the next section).

6.11.1. Configuring Your External Ethernet Adapter

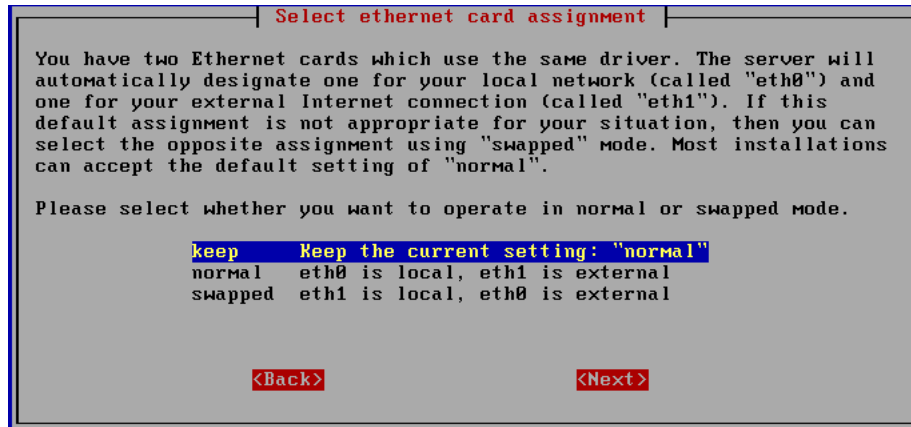
As you did previously with your local ethernet adapter, you need to configure the driver for your external ethernet adapter. As before, the software will attempt to detect the card. If it correctly identifies the card, you can proceed using Option 1, "Keep current driver". If it does not, you will need to manually select the driver.



6.11.2. Assigning Your Ethernet Adapters to Network Connection

To communicate successfully, your server needs to know which ethernet adapter connects it to the internal network and which adapter connects it to the external network/Internet. Your server will make this designation automatically - the first ethernet adapter (in position "eth0") will normally be assigned to the local, internal network and the second ethernet adapter (in position "eth1") will normally be assigned to the external network/Internet. In the event that this assumption is incorrect, this screen allows you to easily swap that designation.

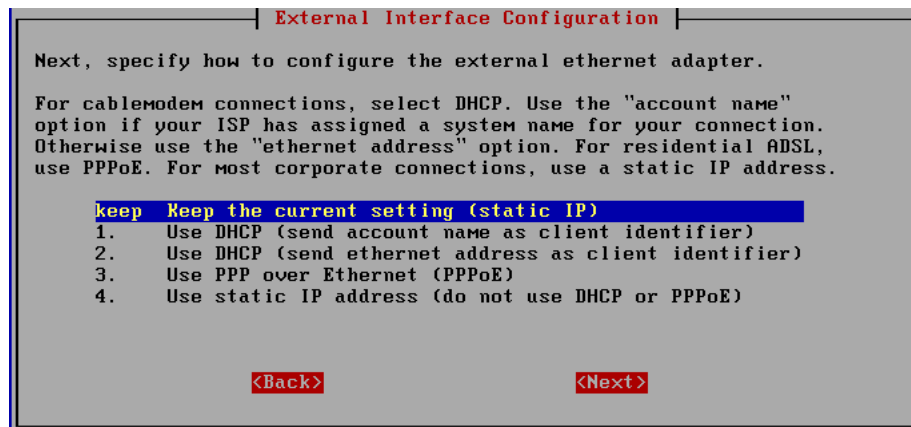
If you don't know which ethernet adapter is designated to eth0 and which is designated to eth1, we suggest you leave it in the default configuration while completing the rest of the screens. You will later have the opportunity to "Test Internet Access" from the server console. If your test fails at that time, return to this screen, swap the card assignment and retry the test.



Tip: If you are using two different network interface cards, you will see which driver is associated with eth0 and which is associated with eth1. This information can help you determine which card is eth0 and which is eth1. If you have two cards that use the identical driver you will see a screen such as the one above where the actual driver is not listed.

6.11.3. Configuring Your External Interface

With a dedicated connection in server and gateway mode, you will be presented with the following screen:



Your server must know three additional things to communicate on the Internet:

- its own unique IP address so that Internet data packets can reach it.
- a subnet mask (also called a netmask) which looks like an IP address and allows other computers to infer your network address from your IP address.
- the IP address of the external gateway for your server. This is the IP address of the router on your server's external network. It identifies the computer that your server should contact in order to exchange information with the rest of the Internet.

Normally, you would need to know this information and enter it into the server console. However, most ISPs are capable of automatically assigning these configuration parameters to your server using a *DHCP server* or *PPPoE*.

If you have a static IP address and your ISP is configuring your server using DHCP or PPPoE, select Option 1, 2 or 3 depending upon how you will be connecting to your ISP. When you first connect to your ISP, your server will automatically be given its external interface configuration parameters.

If your ISP is providing you with a dynamic IP address, the ISP will configure this through DHCP or PPPoE and your server will be re-configured automatically whenever your IP address changes. If you plan to use a Dynamic DNS service, select Option 2. Otherwise, select Option 1.

There are some very good reasons to use a dynamic DNS service if you have a dynamically assigned IP address. It is a simple, affordable way to ensure continuity of service when your IP address changes. Please read the next section on dynamic DNS for more information about dynamic DNS.

If you are using ADSL and need PPP over Ethernet, choose Option 3. You will then be asked for the user name and password you use to connect to your ISP. Note that some ISPs require you to enter their domain name as well as your user name.

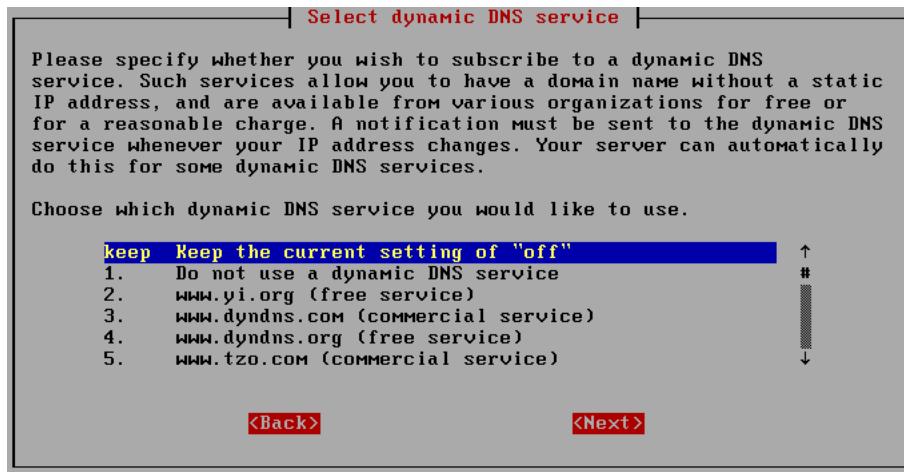
What is PPPoE?

PPPoE is the *Point-to-Point Protocol over Ethernet*. Essentially, it is an implementation of the popular PPP protocol used for dialup connections - only configured to run over an Ethernet connection. Many ISPs that provide ADSL connections use PPPoE as the method of connecting their customers to the Internet over ADSL.

If you have a static IP address and your ISP does not offer DHCP or PPPoE, then your ISP will give you the static IP address, subnet mask (or netmask), and the gateway IP address of the device that your server should connect to in order to communicate with the Internet. Assuming you have this information on hand, you can go ahead and select Option 4. Successive screens will prompt you to enter each parameter.

6.11.4. Configuring Dynamic DNS

If you choose either of the DHCP options or PPPoE, you will be presented with an additional screen where you can choose which dynamic DNS service you wish to use.



The server is pre-configured to operate with four dynamic DNS organizations: yi.org (<http://www.yi.org/>), dyndns.com (<http://www.dyndns.com/>), dyndns.org (<http://www.dyndns.org/>), and tzo.com (<http://www.tzo.com/>). (You can elect to use a different service, but doing so would require some customization of the server.) Once the service is selected, the subsequent two screens will prompt you to enter your account name and the password for your account. (These two parameters would be given to you by the service. Note that the dynamic DNS service may place restrictions on which domain name you can use for your company.) Please read Appendix B on dynamic DNS for more information about whether a dynamic DNS is right for you.

Tip: ServiceLink subscribers do not need to worry about a dynamic DNS service as DNS service is provided as part of the base ServiceLink subscription.

6.12. Configuring the Server for Server and Gateway Mode - Dialup Access

If you select dialup access, successive screens will ask you for the following information:

- information regarding the modem or ISDN connection with your ISP, such as the serial port your modem is connected to ¹
- modem or ISDN initialization screen - most users can simply leave this blank, but with some particular modems or ISDN cards, additional information may need to be entered here
- the dialup access phone number
- username
- password
- connection policy

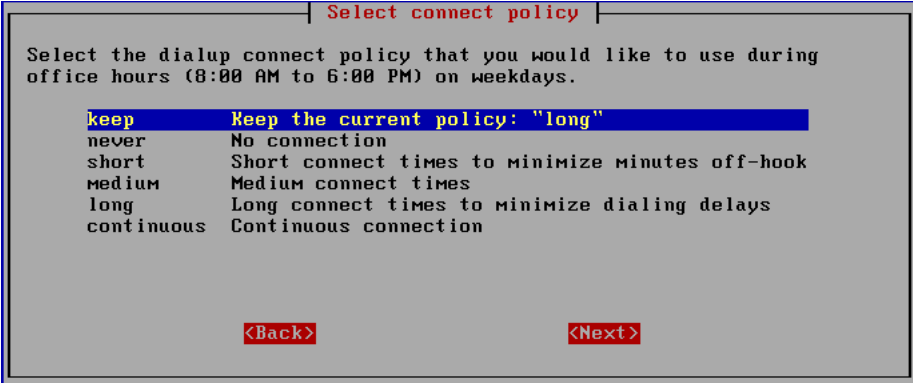
1. Your modem documentation may indicate which serial port is used by the modem. You may also be able to visually identify which port your modem uses.

This last item may be of special interest. As shown in the screen below, you can configure what type of policy you wish to have in place during typical work hours. If you are in a small office and wish to share your phone line between your computer and phone or fax, you may wish to minimize the time you are online. This is also true if your ISP charges a fee on a per-minute basis. On the other hand, if you have a separate phone line or unlimited time with your ISP, you might want to have long connection times or a continuous connection.

Warning

If you are using a dial-on-demand link to your ISP, please be aware that you can incur very steep phone charges due to dialup connection attempts to the ISP. We are aware of at least one case in which a failed modem link at the ISP resulted in several thousand connection attempts over a couple of days - and a hefty phone bill. If your telephone carrier charges you per-call or per-minute fees, we suggest that you contact your ISP and ask whether it is willing to assume responsibility if a failure at their end results in a large phone bill.

After configuring this policy for "work" hours, you can then configure the policy for time outside of office hours and additionally for the weekend. Notice that you do have the choice of *never* , which would allow you to restrict your system from connecting on weekends or during off-hours.



The connection policy defines several choices including Short, Medium or Long. These specify how long the server should wait before disconnecting the dialup connection. If your office only shares a single phone line, the *Short* option minimizes the amount of connection time and frees up the phone line for later use. The down side to this is that if someone is reading a long page on the web site or steps away from their computer for a brief moment, when they want to then go to another web page, the server will probably have disconnected and will need to redial and connect. On the other hand, setting the *Long* connection time will result in users experiencing fewer delays while waiting for the server to reconnect. However, the phone line will used for a larger amount of time.

There are two separate timeout values configured by each choice. One value is the length of time since the last HTTP (web) packet went through the server. The other is a more general timeout for any other types of packets. The difference is there because it is assumed that people reading a web page may take longer to go on to another web page, whereas users connecting to another service (such as ssh or POP3 to an external server) probably will be more active than someone using a web browser. The timeout values are shown in the table below.

Choice	HTTP Timeout	Other Timeout
Short	3 minutes	30 seconds
Medium	10 minutes	5 minutes
Long	20 minutes	10 minutes

Note that there is also the option for a Continuous dial-up connection. Choosing this option is basically equivalent to creating a permanent or dedicated connection, but only doing so through the use of a dial-up connection and a modem or ISDN adapter. One example of this use might be to set a Continuous connection policy during work hours and then some variable policy during off-hours and the weekend. Assuming that your ISP is okay with this arrangement and you can afford to do so financially, these settings would give your users the fastest response time as the connection would always be online.

6.13. Configuring Your DHCP Server

You now will be prompted regarding DHCP service. Your SME Server V5 with ServiceLink can be configured to **provide** DHCP service to your internal network. The DHCP server can automatically configure the other computers on your internal network with such parameters as non-routable IP address, subnet mask and gateway IP address. This reduces the risk of error and simplifies the process of configuring your network.

We recommend configuring your server to use DHCP to configure all of your network clients. You should *not* do this if there is an existing DHCP server on your network as there should typically be only one DHCP server per network.

Select DHCP server configuration

Please specify whether you would like this Mitel Networks Server to provide DHCP service to your local network. This will let you assign IP addresses to your other network computers automatically by configuring them to obtain their IP information using DHCP.

☒ **Keep the current setting: "On"**
☐ Provide DHCP service to local network
☐ Do not provide DHCP service to local network

6.13.1. Configuring the DHCP Address Range

Before the DHCP server is able to assign IP addresses to the computers on your network, you need to tell it what range of IP addresses it can safely distribute. **As above, this section is pre-configured with defaults that are appropriate in most situations. If you have fewer than 180 machines on your local network and no reason to prefer one range of IP addresses over another, you can simply accept the defaults for these screens.**

If the defaults are not appropriate to your situation, you may need a bit of background to understand how to configure this range. For example, if you entered the server address of 192.168.1.1 and subnet mask of 255.255.255.0 (the default settings), the configuration script will infer that your "network" is 192.168.1.0 and that valid addresses are from 192.168.1.1 to 192.168.1.254. If you entered some number such as 192.168.100.1 for the server, the script will infer that your valid addresses will be 192.168.100.1 through 192.168.100.254.

If you enter the number "192.168.202.65" as the "beginning of DHCP address range", as shown below, the first computer served by the DHCP server would receive the IP address of 192.168.202.65. The second computer would receive the IP address of 192.168.1.66, and so on.

Select beginning of DHCP host number range

You must reserve a range of host numbers for the DHCP server to use. Please enter the first host number in this range here. If you are using the standard Mitel Networks SME Server defaults and have no particular preference, you should keep the default values.

192.168.202.65

If you specify that the end of the range is "192.168.202.250", as shown below, then the last computer able to receive DHCP service would be assigned the IP address 192.168.202.250. Once all the available IP addresses within that range are assigned, your DHCP server will no longer serve IP addresses to new computers.

Select end of DHCP host number range

You have selected 192.168.202.65 as the beginning of the range of host addresses for the DHCP server to use.

Please enter the last host address in this range here. If you are using the standard Mitel Networks SME Server defaults and have no particular preference, you should keep the default value.

192.168.202.250

6.13.2. Important issues about the DHCP address range

The usual range maximum is 254: Normally the "end of DHCP address range" cannot exceed "254". If you have more than 253 computers on your network and would like to exceed this range maximum, you can use a Class B or Class A non-routable address for your network. In this case the number entered in the "end of range" field needs to be calculated and entered a little differently. If you fall into this category, we recommend you contact Mitel Networks Corporation or a Mitel Networks Corporation authorized reseller for assistance. Note that the default range maximum is 250. As explained below, this is to allow a few static addresses at the end of the range.

The local IP address assigned to your server itself must fall outside of this range: In other words, you should not assign your server a non-routable IP address that is also assignable by the DHCP service to another computer on your network. If your server is assigned the IP address of "192.168.1.1" then the lowest possible number in the DHCP range should be "2".

We recommend that you leave a small pool of IP addresses that can be manually assigned: Some of the computers (or devices such as network printers) on your network may not be able to accept DHCP service. Therefore, it is preferable to exclude some IP addresses from the DHCP range so they are available to be assigned manually to those computers. For example, using the 192.168.1.0 block of addresses, the default "beginning of DHCP address range" is "192.168.1.65". This ensures that non-routable IP addresses "192.168.1.2" through "192.168.1.64" are available to you if

any computers on your network cannot accept DHCP service. Additionally, the default end of "192.168.1.250" leaves addresses "192.168.1.251" through "192.168.1.254" available.

6.14. Further Miscellaneous Parameters

There are a few, final connectivity-related parameters that must be entered into your SME Server V5 with ServiceLink.

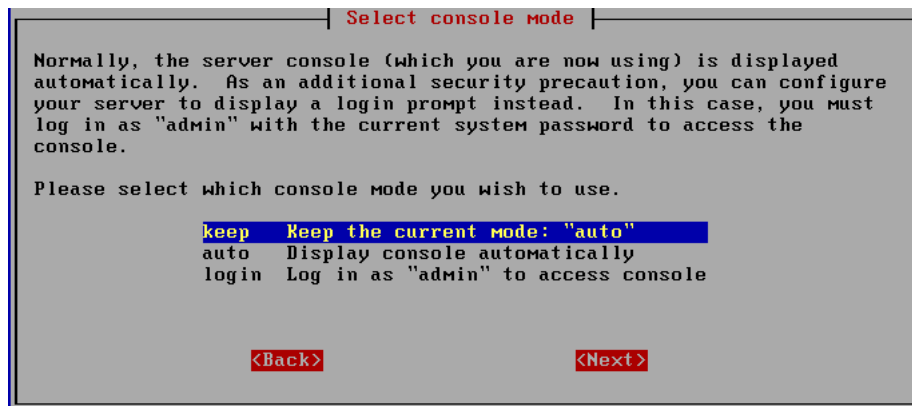
Master DNS server: The first option is for a master (or primary) DNS server. You should only configure this value if your server is behind a firewall and cannot perform direct queries to Internet DNS servers. Most installations should leave this setting blank. You **do not** need to configure your server to use your ISP's DNS servers.

Note: Your SME Server V5 with ServiceLink contains a fully functional caching DNS server and in almost all cases you will *not* need to enter the address here for a DNS server. However, some corporate firewalls restrict DNS queries from internal DNS servers. If that is the case, you will need to supply the address for an external DNS server.

External proxy server: The next screen allows you to configure your server so that the computers on your network will use a proxy server *outside of your own network*. Some Internet Service Providers may require this. Additionally, if your server is behind another firewall, it may need to use the external proxy server. If you have questions about whether to use a proxy server, we recommend you read Appendix C on using a proxy server. In most environments you can probably leave this blank.

Status reporting: You will be asked to decide whether to enable status reporting to Mitel Networks Corporation. Through status reporting, Mitel Networks Corporation, tracks the performance of its servers worldwide. Every day, your server would send a small packet of data containing up-time information to Mitel Networks Corporation. The information sent to Mitel Networks Corporation is minimal and is not shared with any other organization.

Console mode: Next, as shown below, you select the security setting for the server console itself - in other words, whether users will require a password to access the server console. If you choose the default, "auto", the server console will be displayed on your server monitor. In many small office or home office situations, this is perfectly acceptable. However, doing so allows anyone with physical access to your server monitor and keyboard to make system-wide changes. If you are concerned about security in your situation, you may wish to choose "login." This setting prevents users from accessing the server console unless they login as "admin" with the system password you set earlier in the process. Note that this setting controls access to the server console only; it does not control whether you (or anyone else) can administer your server using the web interface.



Contact e-mail address: Finally, you will have the option of providing a contact e-mail address and name. If you would like to be notified of security updates or new versions of software, we strongly encourage you to provide at least your e-mail address. As the screen indicates, we will *only* send you notices of updates and no other information. Your contact information will not be shared.

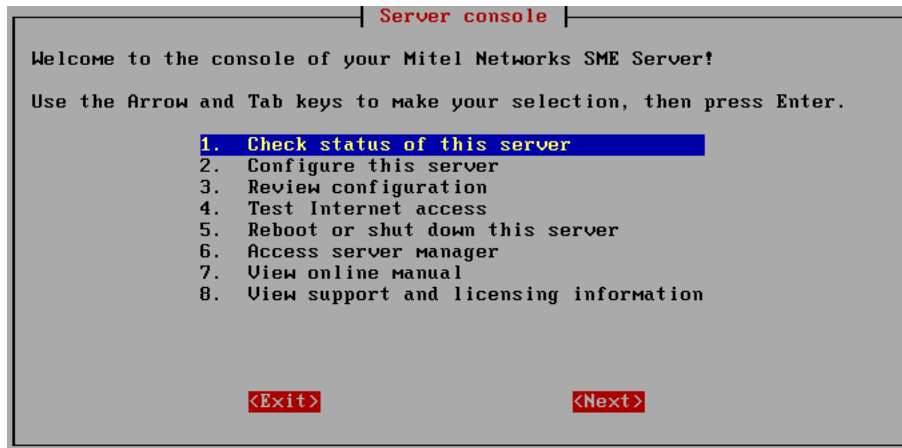
The last screen asks you to confirm the changes you have made. After the changes take effect, you will see other services starting up. When that is finished, your server should be fully operational!

Congratulations - you have configured your SME Server V5 with ServiceLink!!

Afterward you may want to test your Internet access using the test option in the server console. If you chose "auto" earlier, the server console remains permanently "up" on your server. Otherwise you would need to login as "admin". Most routine administration (for example, adding or deleting e-mail addresses) is done from your desktop computer using the web-based server manager (reviewed in a later chapter). Therefore, once it is up and running, most users put their server in an out-of-the-way place and turn off the monitor.

Chapter 7. The Server Console

When installation is complete and if you set server console mode to "auto", the opening screen of the SME Server V5 with ServiceLink server console will appear:



If you set the server console mode to "login", you will be given a login prompt. After you enter the user name "admin" and your system password, you will see the server console screen above.

Note: Any time that you login to your system as the "admin" user you will see the server console. This is true even when connecting to the server remotely using a tool such as *ssh* (discussed later in the chapter on Remote Access).

The server console provides you with basic, direct access to your server. From the server console you can get the following information and perform the following tasks:

Option 1: Provides you with uptime information about your server.

Option 2: Allows you to view and modify the configuration information you entered during the original installation (ethernet cards, IP address information, DHCP, DNS, domain names, etc.)

Option 3: Provides you with a summary of the configuration parameters entered into your server.

Option 4: Allows you to test your Internet access by sending a small test packet of information to a server on the Internet (located at Mitel Networks Corporation) which will confirm that your server is communicating on the Internet.

Option 5: Allows you to smoothly reboot or shut down your server.

Option 6: Provides you with a means to access the web-based server manager using a text-based browser. This is the same interface to which you can connect from another system using a normal graphical browser. This option merely allows you to perform these functions directly from the server console.

Option 7: Connects to <http://www.e-smith.org/docs/manual/> to allow you to read the online version of this user guide.

Option 8: Displays the GNU General Public License (the license governing the distribution and use of SME Server V5 with ServiceLink software) and information on how to contact Mitel Networks Corporation for support.

7.1. Using the Text-based Browser

For Option 6, *Access server manager with text-mode browser*, the server uses a text-based browser called *lynx* to allow you to access the web-based server manager from the server console. Navigation is primarily with the arrow keys - up and down to move through the page, right arrow to follow a link, left arrow to go back. Lynx has a wide range of other commands which you can learn about through the online help available at <http://www.lynx.browser.org/> (<http://www.lynx.browser.org/>) Note that for security reasons some regular features of lynx are *disabled* when you are browsing from the server console (such as the ability to specify an external URL). Type 'q' (for 'quit') to exit the text-based browser.

7.2. Accessing the Linux Root Prompt

If you are an expert user and would like to do advanced modifications to the configuration of your server, you can access the Linux operating system underlying the SME Server V5 with ServiceLink software by logging in as the user "root". If your server is displaying the server console and not a login prompt, you can press Alt-F2 to switch to another screen with a login prompt. To switch back, press Alt-F1. You should always ensure that you log out from the root account when you are finished and before you switch back to the server console.

The password for the "root" user is whatever password is currently set for the administrator of the server. Note that this is the *same* password as that used by the "admin" user account.

Be aware that this ability to switch between the server console and a login prompt is only available when you have physical access to the server. If you connect in remotely as the "admin" user and see the server console, you will *not* be able to switch to a login prompt in that window. (You can, however, open up another remote connection to your server and login as the "root" user.) Note that remote administrative access is *disabled* by default and must be specifically enabled through the Remote Access panel of the server manager.

Note: If you are not familiar with working from the Linux prompt, you may be interested in trying a file management tool called Midnight Commander. It allows you to perform many file operations through a menu-driven interface. Simply type **mc** at the command prompt. Press the function key "F1" for help and "F10" to quit.

Chapter 8. Configuring the Computers on Your Network

8.1. What Order to do Things

For efficiency, we recommend you configure your desktop computers in the following order:

- Step 1:** First, configure one of your desktop computers to work with TCP/IP (using the information in this chapter).
- Step 2:** With TCP/IP up and running on one of your computers, you can now access the server manager over the web and create your employees' user accounts. The next chapter, On-going Administration Using the server manager, explains this simple process.
- Step 3:** Once e-mail accounts are created, you can ensure that all the computers on your network are configured for TCP/IP, e-mail, web browsing and LDAP (using the information in this chapter).

Note: If you already have e-mail accounts set up with your ISP, you will need to do things in a different order to ensure continuous e-mail service to your site. See our online HOWTO document titled *Transitioning From a Prior E-mail System* available at <http://www.e-smith.org/docs/howto/emailtransition-howto.html>

This chapter helps you configure software and hardware supplied by other companies and for that reason is not as specific as the rest of this guide. Given the wide range of computers, operating systems and software applications, we cannot accurately explain the process of configuring each of them. If your computers and applications came with manuals, they might be useful supplements to this chapter. Technical problems encountered in networking your desktop computers and applications are best resolved with the vendors who support them for you.

Important: This chapter demonstrates only *one* of the many possible ways to configure your client computers and is provided here as an example. You should consult with your authorized reseller to determine the most appropriate ways to configure your client computers.

8.2. Configuring Your Desktop Operating System

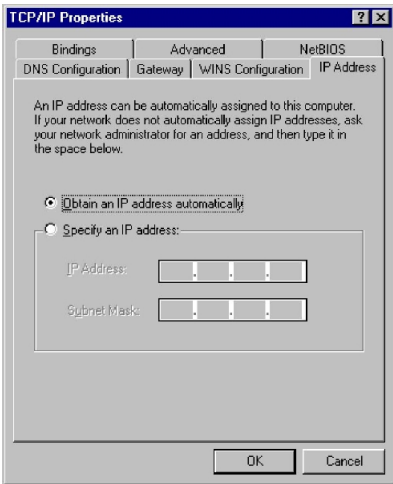
The dialog box where you configure your desktop differs from operating system to operating system and version to version. As an example, in Microsoft Windows 95 or 98, client configuration occurs in the "Properties" dialog box associated with the TCP/IP protocol for your ethernet adapter. To get there, go to the "Control Panel" and select "Network". If a TCP/IP protocol is not yet associated with your ethernet adapter, you may need to add one before you can configure its properties with the following information.

Note: For a more complete example of configuring a Windows 95 client, see our HOWTO document online at <http://www.e-smith.org/docs/howto/wintcpip-howto.html>

Item	Description	What to enter
enable TCP/IP protocol	All your computers must communicate on the network using the TCP/IP protocol.	In Windows you add a TCP/IP protocol. In Apple, open TCP/IP Control Panel.
disable non-TCP/IP protocols	Unless an application relies on a non- TCP/IP protocol, disable all other protocols.	Turn "off" other networking protocols (e.g. NetBeui, etc.)
enable DHCP service	See section below	In Windows, enable "Obtain an IP address service automatically". In Apple, select "DHCP server".

Note: We **strongly** recommend that you configure all clients machines using DHCP rather than manually using static IP addresses. Should you ever need to change network settings or troubleshoot your network later, you will find it much easier to work in an environment where addresses are automatically assigned.

On a Windows 95/98 system, the window will look like the image below.



8.2.1. Automatic DHCP Service

Your server provides a DHCP server that assigns each of the computers on your network an IP address, subnet mask, gateway IP address and DNS IP address(es). For a more detailed explanation of DHCP, consult the section in the Chapter 5 called "Configuring Your DHCP Server".

Note: In some rare cases, you may want to use a static IP address for a particular client machine. The typical approach is to manually enter this IP address into the network properties of the specific machine. The negative side of this approach is that you cannot easily change or alter network settings without having to go in and modify the information on the client machine. However, it is possible to provide this static IP address directly through DHCP rather than manually configuring the client computer. To do so, you will first need to determine the Ethernet address of the client computer (usually through the network properties). Next you will go to the Hostnames and addresses web panel of the server manager and enter the information there.

Only One DHCP Server

It is imperative that no other DHCP server is on your network. If a former DHCP server configured your computers, you should remove that DHCP server from your network. Leave DHCP enabled, and reboot each computer. New IP addresses, netmasks, gateway IP addresses and DNS addresses will be assigned automatically by the server DHCP server.

8.2.2. Manual entry for computers not using DHCP service

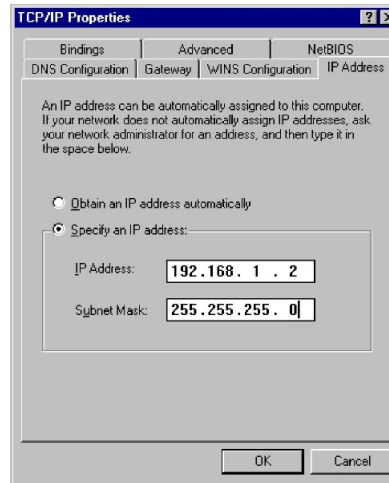
As noted above, we strongly recommend that you perform all your client configuration using DHCP. It is even possible to assign a static IP address through the Hostnames and addresses web panel of the server manager that will be distributed through your DHCP server.

However, if your computers do not support DHCP, you must manually enter the following information into your TCP/IP properties:

Item	Description	What to enter
IP address	Manually enter this information (see paragraph below).	You must assign a different, unique IP address to computers not accepting DHCP (see note below).
subnet mask (or netmask)	Manually enter this number.	The default subnet mask (or netmask) is "255.255.255.0".
gateway IP address	Enter the IP address for the server or, in the case of server-only mode, enter the IP address for your network's gateway (e.g. the firewall or network router).	If you are running in server and gateway mode, your server is your local network's gateway. Enter its IP address here: the default is "192.168.1.1". If you are running in server-only mode, enter the IP address for the device interfacing with your external network.
IP addresses of your domain name servers	Manually enter this information.	Normally you would just add the IP address for your server - the default used in the server console is "192.168.1.1". If you have a firewall other than your server that restricts internal queries to Internet DNS servers, you may need to enter additional DNS servers here.

It is critical that every computer on your network has a unique IP address and that you don't assign two computers the same address. In enabling

DHCP service in the server console, you designated a range of IP addresses for DHCP assignment. You also allocated a block of IP addresses for manual assignment. If you accepted the defaults pre-configured into the server console, IP addresses 192.168.1.2 through 192.168.1.64 will have been set aside for manual entry. To avoid duplication, use only those IP addresses when manually assigning IP addresses to your computers.



After configuring the TCP/IP parameters, you may need to reboot your desktop computer to implement the configuration changes. (For example, most Windows systems need to be rebooted after the TCP/IP configuration has been changed.) Once the settings take effect, your computer will be connected to the server and to the Internet.

8.2.3. MS Windows workgroup configuration

If you are using a Microsoft operating system, you must ensure that your workgroup is the same as the workgroup name of your server. (The default workgroup name is your domain name. In a subsequent chapter, we'll explain how this can be changed using the web-based server manager.) If you are using the default name, go to the Control Panel, select "Network" and then select "Identification". In the field for "Workgroup", type your domain name.

A word about domain names

Once you've set up your server, there's typically a delay of one or more days before your ISP publishes your domain address records (the domain name or names and the associated numerical IP address) so that the information is accessible to other computers on the Internet. Until it does, incoming mail won't be able to find you and computers elsewhere on the Internet won't be able to contact your server using your domain name (for example, www.yourdomain.xxx). However, on your local network you should be able to connect to your server using the short names of 'www' (for web access) and 'mail' (for e-mail clients).

8.3. IMAP versus POP3 e-mail

There are two common standards for e-mail management, IMAP and POP3. Your server supports both protocols. You will need to select the protocol that is right for your organization.

POP3 is the earlier, better-known e-mail protocol. POP3 was designed to permit on-demand retrieval to a single client machine. E-mail is stored on the mail server until you retrieve it, at which time it is transferred over the network to your desktop machine and stored in your e-mail box there.

Benefits of POP3	Drawbacks of POP3
Even when you are not connected to your network, you have access to the e-mail stored on your desktop.	POP3 was not originally intended to support users accessing and managing their e-mail from remote systems. Because your e-mail is stored on your desktop, setting up remote access of your e-mail when you are at a different computer can be complex.

IMAP e-mail, in contrast, is designed to permit interactive access to multiple mailboxes from multiple client machines. You manage your e-mail on the mail server over the network. You read your e-mail over the network from your desktop, but the e-mail is not stored on your desktop machine - rather, it is permanently stored and managed on the server.

Benefits of IMAP	Drawbacks of IMAP
------------------	-------------------

Benefits of IMAP	Drawbacks of IMAP
You can access all of your new and stored e-mail from any machine connected to a network. Because all employee e-mail is stored on the server, backup of e-mail is easily accomplished.	If you are not connected to a network, new and stored e-mail messages are not available to you.

8.4. Configuring Your E-mail Application

Each user’s e-mail application requires information about that user’s account, where to send outgoing e-mail and pick up incoming e-mail. This information is usually entered in the "preferences" or "options" section. Most e-mail applications require you to enter the following information:

User’s e-mail address: The user’s e-mail address is the user account as created in the server manager plus the @domain name. Typically it will be in the form of *username@yourdomain.xxx* (e.g. *afripp@tofu-dog.com*).

E-mail server or outgoing e-mail SMTP server: This is the name of the e-mail server from the server. Normally you should just enter **mail** here. If you prefer, you should also be able to use the full domain name of *mail.yourdomain.xxx* (e.g. *mail.tofu-dog.com*).

E-mail account name or user name: this is the name before the @ in the e-mail address. For example, the username for "*afripp@tofu-dog.com*" is "*afripp*".

If you choose POP3 e-mail service:

Enable POP3 protocol: Typically, to enable the POP3 protocol for incoming e-mail, you click on the POP3 checkbox or select POP3 from a pull-down menu in the section of your e-mail application dedicated to the incoming e-mail server.

Disable IMAP protocol: To disable the IMAP protocol for outgoing mail (not all e-mail applications have IMAP protocol) click the IMAP checkbox "off".

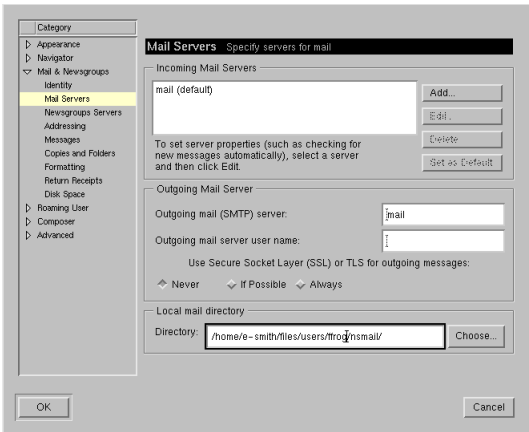
Delete read e-mail from server: We recommend you configure your e-mail application so e-mail that has been read is not left on the server. To do this, click off the checkbox marked "leave mail on server" or click on the checkbox marked "delete mail from server".

If you select IMAP e-mail:

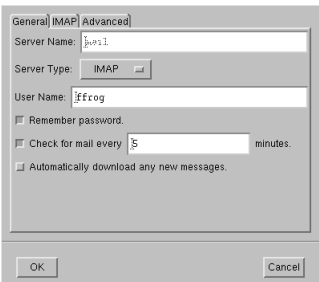
Enable IMAP protocol: Typically, to enable the IMAP protocol for incoming e-mail (note that not all e-mail applications offer IMAP support) you click on the IMAP checkbox or select IMAP from a pull down menu in the section of your e-mail application dedicated to the incoming e-mail server.

Disable POP3 protocol: To disable the POP3 protocol for outgoing mail, click the POP3 checkbox "off".

The images below show you the sequence in Netscape. First you choose *Preferences* from the *Edit* menu and click on *Mail Servers* as shown in:



If you have not configured a mail server yet, you will need to press the *Add...* button and enter information about your server. Otherwise, you will select the default mail server listed and click on the the *Edit...* button. This will bring up a screen where you enter the user name and choose whether you are using IMAP or POP3:



Netscape should now be ready to send and receive e-mail.

8.5. Configuring Your Web Browser

Most browsers are configured using a dialog box called "preferences", "network preferences" or "options". Some browsers need to be configured to access the Internet either directly or via a proxy server. When required, most desktop applications, your web browser included, should be configured as though they were directly accessing the Internet. Although the server uses a security feature known as IP masquerading, thereby creating an indirect connection to the Internet, this is a transparent operation to most of your desktop applications. Hence, you should ensure that the "Direct connection to the Internet" check box is clicked "on" in your web browser.

Under certain circumstances, using a proxy server can improve the perceived performance of your network. The server includes HTTP, FTP and Gopher proxy servers. Normally, we recommend these be disabled in your browser.

If you decided that you *do* want to use proxy servers ¹, you will need to enter the IP address or domain name of the proxy server (i.e. your server) into the configuration screens of your web browser. The port number you will need to enter to connect to the proxy server is 3128. This information is the same for HTTP, Gopher and FTP proxying.

The image below shows how a proxy server would be configured in Netscape Navigator.

You may configure a proxy and port number for each of the internet protocols that Netscape supports.

FTP Proxy: Port:

Gopher Proxy: Port:

HTTP Proxy: Port:

Security Proxy: Port:

WAIS Proxy: Port:

You may provide a list of domains that Netscape should access directly, rather than via the proxy:

No Proxy for:

SOCKS Host: Port:

OK Cancel

8.6. Configuring Your Company Directory

Your SME Server V5 with ServiceLink will automatically create a company directory and update it as you maintain your e-mail accounts. The next chapter explains how to configure this service. Any client program that uses LDAP (Lightweight Directory Access Protocol), such as the address book in Netscape Communicator, will be able to access the directory. For example, with Netscape, look under the "Communicator" menu and choose "Address Book". Then look under the File menu and select "New Directory". You will see a dialog box similar to the one shown here.

Name:

Description:

LDAP Server:

Server Root:

Port Number:

Maximum Number of Hits:

☐ Secure

☐ Login with name and password

☐ Save Password

OK Cancel

You will need to enter the following information:

1. Note that laptop users should disable proxy servers when working away from their local area networks.

- Enter the name you wish to give your company directory - any name will do.
- The LDAP server is the name of your web server, in the form `www.yourdomain.xxx`.
- The Server Root information can be found on the "Directory" screen in your server manager (more information on this is available in the next chapter). The usual form, assuming your domain is `yourdomain.xxx`, is `dc=yourdomain,dc=xxx`. (No spaces should be entered between the "dc=" statements.)
- The Port Number is always 389.

Once the address book has been created, Netscape can display a list of all e-mail accounts if you type an asterisk into the search field and press "Enter".

Chapter 9. On-going Administration Using the server manager

The server manager is a simple control panel that allows you to administer your network. Using the server manager, you perform such tasks as adding or deleting e-mail addresses, setting the system date and time, and creating a starter web page. The server manager is accessed through a web browser by visiting the URL <http://www.yourdomain.xxx/server-manager> or more simply <http://www/server-manager>. The staff at The Pagan Vegan would access the server manager using the URL <http://www.tofu-dog.com/server-manager>. We recommend you bookmark this address so that you can return to it whenever you wish to access the server manager.

Note: For security reasons, you are only able to access the server manager through a web browser *on the local network*. Remote access is only possible using remote access tools such as ssh and PPTP.



When you arrive at the correct URL, you'll be asked to enter your user name (which is always "admin") and the password you created during the installation process. Enter that information and click "OK" to be taken to the server manager. It will look like the screen shown above.

In the next four chapters, we'll explain each of the administrative functions in the order in which they appear in the frame running down the left side of the screen. The links are grouped together under four headings: Security, Configuration, Collaboration and Miscellaneous.

Note: As even one further layer of security, you can also connect to the server manager using the secure HTTPS protocol. This establishes an encrypted channel of communication between your browser and the server, even on your local network. To connect to the server manager in this manner, use a URL prefix of "https" as in the example: <https://www.yourdomain.xxx/server-manager>.

Chapter 10. Security

10.1. Password

This screen lets you change your system password at any time. To do so, type the new password in the first field. Verify the new password by entering it in the second field. (Your password can be any combination of printable characters, including upper- and lower-case letters, numbers, and punctuation marks.) If you make a mistake, click the "Back" button on your browser and try again. Note that whenever you change your password, the system will prompt you for the revised password as soon as you access another feature. When you get the "Authorization Failed" message, click OK, enter the new password and press "Enter".

Change system password

Certain services on this Mitel Networks server installation require a username and password (for example this web page for the server manager application). The username is always **admin**. You can change the system password using the fields below.

New system password:

New system password (verify):

10.2. Remote Access

If you're an advanced user, the SME Server V5 with ServiceLink provides several different ways to access the underlying operating system, either from a computer on your internal network or from a computer outside your site on the Internet. Additionally, you have the ability to access your computer network securely from a remote computer. All of these operations are configured from the screen shown below in the server manager.

Change remote access settings

For each of the options below, the **private** setting allows anyone from your local network to access your Mitel Networks server. The **public** setting allows access from anywhere on the Internet. The **no access** setting disables access. To understand the security implications of changing these options from the default settings, you should read the user's guide section on remote access.

You can control **secure shell (openssh)** access to your Mitel Networks server. The public setting should only be enabled by experienced administrators for remote problem diagnosis and resolution. We recommend leaving this parameter set to **no access** unless you have a specific reason to do otherwise.

Secure shell (ssh) access:

Allow administrative command line access over ssh:

Allow ssh access using standard passwords:

You can allow **PPTP** access to your Mitel Networks server. You should leave this feature disabled by setting the value to number 0 unless you require PPTP access.

Number of PPTP clients:

You can also control **FTP** write access for the admin and user accounts on this server. (Write access is never permitted via anonymous FTP or via the information bay accounts.) We strongly recommend leaving this parameter set to **private** unless you have a specific reason to do otherwise.

FTP user account access:

Note: this policy limits access to the FTP server and overrides other settings, including those for individual information bays.

FTP access limits:

You can also control **telnet** access to your Mitel Networks server.
WARNING: telnet is inherently insecure and should only be used in circumstances where no practical alternative exists. You should leave this option set to **no access** and use the [secure shell](#) if remote access is required.

Telnet access:

Each of these remote access methods is described below.

10.2.1. ssh

If you need to connect directly to your server and login from a remote system belonging to you, we *strongly* encourage you to use ssh instead of telnet. In addition to UNIX and Linux systems, ssh client software is now also available for Windows and Macintosh systems. (See the section below.)

If you do not have any reason to allow remote access, we suggest you set this to **No access**.

ssh (secure shell)

ssh (secure shell) provides a secure, encrypted way to login to a remote machine across a network or to copy files from a local machine to a server. Many people do not realize that many programs such as telnet and ftp transmit your password in plain, unencrypted text across your network or the Internet. *ssh* and its companion program *scp* provide a secure way to login or copy files. The ssh protocol was originally invented by SSH Communications Security which sells commercial ssh servers, clients, and other related products. The protocol itself has two versions - SSH1 and SSH2 - both of which are supported by most clients and servers today. For more information about SSH Communications Security and its commercial products, visit <http://www.ssh.com/>.

OpenSSH, included with the SME Server V5 with ServiceLink, is a free version of the ssh tools and protocol. The server provides the ssh client programs as well as an ssh server daemon and supports both the SSH1 and SSH2 protocols. For more information about OpenSSH, visit <http://www.openssh.com/> (<http://www.openssh.com/>).

Once ssh is enabled, you should be able to connect to your server simply by launching the ssh client on your remote system and ensuring that it is pointed to the external domain name or IP address for your server. In the default configuration, you should next be prompted for your user name. After you enter *admin* and your administrative password, you will be in the server console. From here you can change the server configuration, access the server manager through a text browser or perform other server console tasks.

If you do enable ssh access, you have two additional configuration options:

- **Allow administrative command line access over ssh** - This allows someone to connect to your server and login as "root" with the administrative password. The user would then have full access to the underlying operating system. This can be useful if someone is providing remote support for your system, but in most cases we recommend setting this to *No*.
- **Allow ssh using standard passwords** - If you choose *Yes* (the default), users will be able to connect to the server using a standard user name and password. This may be a concern from a security point of view, in that someone wishing to break into your system could connect to your ssh server and repeatedly enter user names and passwords in an attempt to find a valid combination. A more secure way to allow ssh access is called *RSA Authentication* and involves the copying of an ssh key from the client to the server. This method is supported by your server, but is beyond the scope of this user guide and will eventually be covered by additional documentation on the e-smith.org web site.

Note: By default, only two user names can be used to login remotely to the server: *admin* (to access the server console) and *root* (to use the Linux shell). Regular users are **not** permitted to login to the server itself. If you give another user the ability to login remotely to the server, you will need to access the underlying Linux operating system and manually change the user's shell in */etc/passwd*.

10.2.1.1. ssh clients for Windows and Macintosh systems

A number of different free software programs provide ssh clients for use in a Windows or Macintosh environment. Several are extensions of existing telnet programs that include ssh functionality. Two different lists of known clients can be found online at <http://www.openssh.com/windows.html> (<http://www.openssh.com/windows.html>) and <http://www.freessh.org/>.

A commercial ssh client is available from SSH Communications Security at: <http://www.ssh.com/products/ssh/download.html> (<http://www.ssh.com/products/ssh/download.html>). Note that the client is free for evaluation, academic and certain non-commercial uses.

10.2.2. PPTP

The *Point-to-Point Tunnelling Protocol (PPTP)* is used to create client-to-server Virtual Private Networks (VPNs) and was developed by the PPTP Forum, an industry group which included Microsoft and several other companies. A VPN is a private network of computers that uses the public Internet to connect some nodes. PPTP allows users to connect to their corporate networks across the Internet.

Microsoft's PPTP implementation is widely used in the Windows world to provide remote access across the Internet. If you have a remote Windows system (for instance, a laptop or a home computer) that has access to the Internet, you can also access the information stored on your server.

If you wish to enable VPN access, you must decide how many individual PPTP clients you will allow to connect to your server simultaneously, and enter that number here. The simplest method is to enter the total number of remote PPTP clients in your organization. Alternatively, if you have a slow connection to the Internet and do not want all of those PPTP clients to connect at the same time, you can enter a lower number here. For instance, if you have five users who from time to time use PPTP to connect remotely, entering 5 here would allow all of them to connect at any time

Entering 2 would only allow two users to connect at any given time. If a third user tried to connect, he or she would receive an error message and would not be able to connect until one of the other users disconnected. If, on the other hand, you entered 0, no PPTP connections would be allowed.

After you enter a number and press Save, the server should be ready to accept PPTP connections.

To connect using PPTP, the protocol must be installed on each remote Windows client. Typically, this is done through the Network Control Panel (you may need to have your original Windows installation CD available). After it is installed (a reboot of your Windows system may be needed), you can create new connections through the Dial-Up Networking panel by entering the external IP address of the server you wish to connect to. Once you're finished, you should be able to initiate a PPTP connection by double-clicking the appropriate icon in the Dial-Up Networking window. When you then open up your Network Neighborhood window, you should see your server workgroup listed there.

Note: Your connection to the Internet needs to be established *first* before you initiate the PPTP connection. This may involve double-clicking one Dial-Up Networking icon to start your Internet connection, then double-clicking a second icon to start the PPTP connection. To shut down, disconnect your PPTP connection first, then disconnect from your ISP.

Warning

To protect your network, the SME Server V5 with ServiceLink enforces the use of 128-bit encryption for PPTP connections, rather than the 40-bit encryption provided in earlier versions of Microsoft's PPTP software. If you are unable to establish a PPTP connection to your server, you should visit <http://windowsupdate.microsoft.com/> (<http://windowsupdate.microsoft.com/>) and download the appropriate update. Due to the dynamic nature of Microsoft's web site, the page may appear differently depending upon the version of Windows you are using. In most cases, you will want to look or search for *Virtual Private Networking* or a *Dial Up Networking 128-bit encryption update*. You may need to install the 40-bit encryption update *first*, and then install the 128-bit encryption update. Note that with Microsoft's *ActiveUpdate* process, if you are not presented with the choice for this update, it is most likely already installed in your system.

10.2.3. FTP

Another way to upload or download files to and from your server is to enable a protocol called FTP, or "file transfer protocol". This screen enables you to set your policy for FTP. Note that allowing liberal FTP access to your server does reduce your security. You have two options that you can set here.

FTP user account access: Private FTP access allows only people on your internal network to write files to your server. Public FTP access allows users both inside and outside your local network to read or write files on your server, provided they have an account and password. If, for example, you want to be able to update your web site from home using FTP, you would choose the "Public" setting. We strongly recommend you leave this as **Private** unless you have a specific reason to do so.

FTP access limits: This allows you to set an overall site-wide policy for FTP access. *The setting you choose here will override all other FTP settings on your server.* For example, if you choose "Disable public FTP access" here and then later configure an i-bay to allow public FTP access from the Internet, such access will be forbidden. Note that one of the choices here allows you to completely disable any use of FTP.

10.2.4. telnet

telnet has traditionally been one of the tools used to login remotely to other systems across a network or the Internet. This screen gives you the options to control the use of telnet as a means of connecting to your server. Telnet can be useful in that it allows you to login remotely and diagnose problems or configure settings. However, when you use telnet, all user names and passwords are transmitted **without any kind of encryption**, dramatically reducing the security of your server. For that reason, we **strongly** recommend the use of *ssh* as described above.

Note: Because telnet has been and continues to be widely used to date, we are providing the ability to use telnet for remote access. However, as *ssh* usage increases, it is our intention to remove telnet access from future releases of the server.

Telnet access: This can be set to "No Access", "Private" or "Public". Because of the inherent security weakness mentioned above, we *strongly* recommend that you leave this set to **No Access** (the default) and instead use *ssh* as described above. If you do need to enable telnet access, we suggest that you enable "public" or "private" telnet access only when absolutely necessary, and disable such access when it is no longer required. If "public" access is enabled, a red warning will appear at the top of every server manager screen.

Note: Because of these security concerns, we do not allow administrative command line access (connecting as 'root') using telnet. Please use *ssh* instead.

10.3. Local networks

Your SME Server V5 with ServiceLink provides services to machines on the local network and it gives machines on that network special privileges and access. For example, only machines connected to the local network can access the mail server on your server to send mail. When you configured your server, you provided it with sufficient information to deduce its own local network. Machines on the network are automatically identified by the server as being eligible for these privileges and access.

If your company only has one network that is being serviced by the server, you do not need to add any information here.

Some advanced users may wish to extend privileges to more than one network of computers. If you would like your server to identify one or more additional networks for those privileges, you will be asked to enter those network IDs and the subnet mask for each network here.

Note that depending on the architecture of your network infrastructure, the instructions for configuring the client machines on that additional network may be different than the instructions outlined in the chapter in this user guide. If you have questions regarding adding another network, you may wish to contact Mitel Networks Corporation or a Mitel Networks Corporation authorized reseller for technical support.

Chapter 11. Configuration

11.1. Set date and time

Accessing this section allows you to set the system date and time either manually or using a network time server. Pull-down menus for month and time zone ensure accurate entry. The server manager will reset the time automatically during daylight savings time. There are worldwide time zones with multiple selections for countries with multiple time zones. (including standard time zones, states/provinces and even cities). This ensures that regional variations in time zones and daylight savings time are accurately reflected.

Date and time configuration

This is where you configure the date and time of this Mitel Networks SME Server. You may use an existing network time server or manually set the date and time for your time zone.

Set Date and Time

Warning: If you have configured a network time server [below](#), do NOT manually set the time or date here. Doing so will break the network time synchronization.

Current setting: **Friday November 23 2001, 2:52:05 AM US/Eastern**

New month/day/year:	November ▾	23	2001
New hour/min/sec:	2	52	05
AM/PM and time zone:	AM ▾	US/Eastern ▾	
Save Date/Time Settings			

Network Time Server

The Mitel Networks SME Server can periodically synchronize the system clock to a network time protocol (NTP) server. To enable this service, indicate so in the checkbox and enter the hostname or IP address of the NTP server below.

Enable NTP Service	<input type="checkbox"/>
NTP server:	<input type="text"/>
Save NTP Settings	

Instead of setting the time manually, you can use a *network time server*. A time server is a device on the Internet that keeps accurate time and is able to communicate the time to other computers over the Internet using the *Network Time Protocol (NTP)*. Many organizations around the world provide Internet time servers for free.

Warning

After you start using a network time server, you should **NOT** set the time or date manually. If you do so, the network time synchronization will no longer function.

This screen in the server manager allows you to configure your server to connect regularly to a time server and synchronize the clock on the server with the time provided by the time server. To do this, simply check the box for "Enable NTP Service", add the domain name or IP address of the time server in the space provided and click "Save NTP Settings". Using a time server is optional but doing so can greatly increase the accuracy of your system.

For more information about using a network time server, visit <http://www.ntp.org/>. You can also find a list of publicly available time servers at <http://www.eecis.udel.edu/~mills/ntp/servers.htm> (<http://www.eecis.udel.edu/~mills/ntp/servers.htm>). You should always use a *secondary* time server (also called a *stratum 2* server) to lighten the load on the primary time servers.

Tip: In order to make sure the network time server is set to your timezone, you should go through this screen once and *manually* set the time to be correct and with the correct timezone. After doing that, go back to this panel and set the server to use a network time server.

11.2. Workgroup

If you are using a computer on a local network and you wish to access the server via Windows file sharing, it is important that you are logged onto the same workgroup as your SME Server V5 with ServiceLink. This screen allows you to enter the name of the Windows workgroup the server

should appear in. You should also enter the Windows server name. In order that you may later connect multiple locations using IPSEC VPNs, we suggest that you use a different name for each server. If you wish you can change the workgroup name to correspond with an existing workgroup. Macintosh users need only enter a server name or accept the defaults.

Change workgroup settings

Enter the name of the **Windows workgroup** that this Mitel Networks server should appear in.

Windows workgroup:

Enter the name that this Mitel Networks server should use for Windows and Macintosh file sharing.

Server name:

Should this Mitel Networks server be the domain master for your Windows workgroup? Typically the answer should be **yes** unless a Windows server is already performing this role on your network.

Domain master: ☐ Yes

Also in this section, you can specify whether the server should be the domain master for your Windows workgroup. Most sites should choose "Yes" unless you are adding an server to an existing network which already has a domain master.

Warning

If you have a Windows NT server or Windows 2000 server on your network that is functioning as a network server, you should most likely answer "no" because that other server will act as the domain master.

If you *do* configure your system to be the domain master, a special Windows share called `NETLOGON` is created with a DOS batch file called `netlogon.bat`. This batch file is executed by Windows clients that have been configured to "Logon to domain". The `netlogon.bat` file we provide by default does very little, but advanced users can, if they wish, modify this script to set environment variables for their clients or provide automatic drive mappings.

As the `NETLOGON` share is only writable by the "admin" user, you modify the `netlogon.bat` script by logging on to a Windows system as "admin", connecting to the share and then modifying the script using a Windows text editor. Be aware that the `NETLOGON` share will not be visible in Network Neighborhood or other similar tools. As the "admin" user, you will need to connect to the share or map a drive to it, by using the specific path:

```
\\servername\NETLOGON\
```

The sample file contains a few examples of setting the system time for each machine and also for mapping a common drive for all Windows client.

11.3. Directory

Your SME Server V5 with ServiceLink provides an easy mechanism for creating a company directory. Each time you create or delete an e-mail account, your directory will be automatically updated with the new information.

Change LDAP directory settings

The LDAP server provides a network-available listing of the user accounts and groups on your Mitel Networks server, and can be accessed using an LDAP client such as the Address Book feature in Netscape Communicator. Configure your LDAP client with the local IP address of your Mitel Networks server, port number 389, and the server root parameter shown below.

Server root: **dc=tofu-dog,dc=com**

You can control access to your LDAP directory: the private setting allows access only from your local network, and the public setting allows access from anywhere on the Internet.

LDAP directory access:

These fields are the LDAP defaults for your organization. Whenever you create a new user account, you will be prompted to enter all of these fields (they can be different for each user) but the values you set here will show up as defaults. This is a convenience to make it faster to create user accounts.

Default department:

Default company:

Default street address:

Default city:

Default phone number:

You can either leave existing user accounts as they are, using the above defaults only for new users, or you can apply the above defaults to all existing users as well.

Existing users:

In this section of the server manager, you specify the default directory information for new accounts - the user's department, company, street address, city and phone number. Each time you create an e-mail account, the fields will contain the information entered here as the default. If you wish, you can change the information for each user.

At any time in the future, you can change the default information and have the new information apply to all new users or to all existing users as well. The field to do this is located near the bottom of the screen. Choosing "update with new defaults" is a convenient one-click method of revising your directory when, for example, your company has moved to a new address.

11.4. Printers

Your SME Server V5 with ServiceLink enables all users on your network to easily share a printer. The printer can be either locally attached to a parallel or USB port on your server or can be a network printer. All the server needs is some basic information: the printer name (which can be anything you want, as long as it starts with a lower-case letter and consists only of lower-case letters and numbers, with no spaces), a brief description (for example, "the printer down the hall") and the location of the printer - whether it's on the network or directly connected to your server through a parallel or USB port.

Create a new printer

Please choose a unique name for the printer and enter a brief description. The printer name should contain only lower-case letters and numbers, and should start with a lower-case letter. For example "hplaser", "epsonlp", and "canonbj" are valid choices, but "HP LaserJet", "Canon BubbleJet", and "HP JetDirect Printer" are not.

Printer name:

Brief description:

Location:

If you choose "Network printer", you will see an additional screen that will ask for the hostname or IP address and the network printer name. Enter that information where requested. For the network printer name, you can use the default setting, `raw`, unless you have some reason to do otherwise. (`raw` is the name used by most network printers for their main print queues.)

Note: For maximum flexibility in making changes later, we suggest that you enter the hostname for a network printer here and enter the IP address

and allowing you to make changes. Note that many modern network printers can be configured automatically. To do so, enter their hostname, IP address and Ethernet address in the Hostnames and addresses panel.

Note also that the server printing system does not perform any filtering and passes the print requests *directly* from the client computers to the printer in the "raw" or "pass-through" machines. For this reason, the SME Server V5 with ServiceLink does not have a list of "supported printers". Most printers are supported as long as the appropriate driver is installed in the operating system on your *client* computers.

However, there are some newer printers that only have a Windows driver available and rely heavily on that operating system to perform their print functions. These printers cannot be used on the server. If you are concerned about whether your printer will work with your server, you can visit Red Hat's Hardware Compatibility List (<http://hardware.redhat.com/redhatready/html/us/static-hcl/intel-input-output.html>) or explore the information found at LinuxPrinting.org (<http://www.linuxprinting.org/>).

As a final item, you should be aware that in order to use the printers available through your server a user must be logged in to their client system with a user name and password that is valid on the server. For instance, if a user is logged in as `tturtle` on their Windows desktop and that user account does *not* exist on the server, the user will *not* be able to print to the printers managed by the server. Either the user will have to logout and log back in as a valid user or the `tturtle` account will need to be created on the server.

11.5. Hostnames and addresses

When you installed your SME Server V5 with ServiceLink, you were asked to provide a name for your system. That name and several other "standard" names are automatically configured in your system's *host table* during the installation process. This host table is consulted as part of the name resolution process. The "Hostnames and address" web panel allows you to modify this table and specify different host "names" for each domain on your system, as well as to control how those names resolve both for systems on your local network and also for systems on the larger Internet.

For instance, when someone tries to connect to "www.mycompany.xxx", they will be taken to wherever "www" has been set to point to. As seen in the image below, this screen in the server manager allows you to view these default settings, and also to modify the configuration.

Using the Hostnames Panel with ServiceLink

Throughout the screens linked to from the Hostnames panel, you will find the text "Publish globally?" with a checkbox next to it. If you are a subscriber to ServiceLink, you have the option of publishing these records through the ServiceLink DNS Configuration and Hosting service. If you select this option, the hostname and IP address information that you enter will be uploaded to the Mitel Networks NOC and published through the global DNS system.

Create, remove, or change hostnames

[Click here](#) to create a new hostname for this Mitel Networks Server.

[Click here](#) to create a new hostname for a local host.

[Click here](#) to create a new hostname for a remote host.

Current list of hostnames for "tofu-dog.com"

Hostname	Visibility (*)	Location	Local IP	Global IP	Ethernet address		
ftp	Local	Self				Modify...	Remove...
mail	Local	Self				Modify...	Remove...
ottawa1 (**)	Global	Self					
www	Local	Self				Modify...	Remove...

(*) – The Mitel Networks SME Server with ServiceLink DNS configuration and hosting service provides the ability to automatically make hostnames available throughout the Internet. To activate this server for ServiceLink, click on the [Status](#) panel.

(**) – This host represents your system name and cannot be modified or removed.

Suppose, for example, your company's web site was hosted at some other location, such as on your ISP's web servers. If you wanted "www.mycompany.xxx" to point to your ISP's server, you would modify the entry here by clicking the "Modify..." link next to "www". The image below shows the screen in which you would perform the task:

Modify hostname

Select whether this hostname is to refer to "Self" (this Mitel Networks Server), "Local" (another server on your local network), or "Remote" (a server outside your local network).

If you select "Self", the only other relevant field is whether to publish the hostname globally. The local IP, ethernet address, and global IP addresses are all ignored, since the Mitel Networks server already knows those values.

If you select "Local", all fields are relevant.

If you select "Remote", the relevant fields are whether to publish the hostname globally, and the global IP address. Whether inside or outside your local network, the hostname points to the global IP address.

Hostname: **www**

Domain: **tofu-dog.com**

Location: ☐

Local IP:

Ethernet address:

The Mitel Networks SME Server with ServiceLink DNS configuration and hosting service provides the ability to automatically make this hostname available throughout the Internet. To activate this server for ServiceLink, click on the [Status](#) panel.

Publish globally? ☐

Global IP:

You would first change the location to "Remote" and then enter the IP address of your ISP's server in the field marked "Global IP".

11.5.1. Creating New Hostnames

Creating new hostnames simply involves selecting one of the links at the top of the Hostnames and addresses panel and filling out the appropriate fields. As mentioned previously, if you are a ServiceLink subscriber you can check "Publish globally?" and your changes will be propagated to the global DNS system automatically.

Note that if your system is configured with any virtual domains, you will have the choice of the domain in which you want to create the hostname. This allows you, for instance, to have "www.tofu-dog.com" pointing to one IP address and "www.mycompany.xxx" pointing to a completely separate IP address.

Note: Beyond your primary domain and any virtual domains you may have configured, ServiceLink subscribers will also have the option of adding hostnames in the special `e-smith.net` domain.

The hostnames you can create on this panel fall into three categories:

Additional names for your server: For instance, you might want to set up "intranet.mycompany.xxx" to point to your server. All you do here is enter the hostname and, if appropriate, choose the domain for the hostname.

Remote hosts: As mentioned in the example earlier, you might want to point a hostname such as "www" to a remote system. While "www" is created by default, you can create other names such as "home", "research", or any other appropriate name. In the form, you simply enter the hostname, choose the domain, and enter the remote IP address.

Local hosts: This screen is a bit more complicated because you have more options. At a basic level, you can create a hostname in a domain that points to another computer on your local network. To do this, just type in the hostname and enter the IP address in the "Local IP" field. For instance, you might want "research" to point to a computer system inside your network.

Where this gets complicated is when you want "research.mycompany.xxx" to be accessible both *inside* and *outside* your local network. The challenge is that your local IP addresses are only accessible *inside* your network. For that reason, the target computer system will need to have two network interface cards - one connected to the internal network and one connected to the external network. You would then enter both IP addresses in this screen in the "Local IP" and "Global IP" fields. Note that this will only work if you are a ServiceLink subscriber as the server alone does not update public DNS information.

Note: The "Ethernet address" field when creating a hostname pointing to a local host is only used for reserving IP addresses through DHCP as mentioned in the next section.

11.5.2. Reserving IP Addresses Through DHCP

Another task you can perform through this panel is to reserve an IP address for a given system based on its Ethernet address. For instance, you might have another intranet web server within your company that you want to always have the same IP address. One method of assigning that address is to manually configure the client machine to have a static IP address. The negative aspect of doing this is that if you later want to change the network settings for that machine, you must manually go and configure that machine. An example would be if one of your DNS servers changed its IP address. Additionally, you have to keep track somewhere of the fact that you have assigned a specific IP address to that machine.

Rather than configuring the machine manually, you can *reserve* an IP address from the DHCP server for that specific machine. This has the same result as manually configuring a static IP address, but offers two benefits. First, you have one location to keep track of all assigned static address. Second, through the DHCP server you will provide network settings. If you wish to change those settings, the change can be simply done on your server. All DHCP clients will then receive those updated changes when they renew their DHCP-provided addresses.

To reserve an IP address, you must first determine the Ethernet address of your client system. Windows NT/2000 users can type the command `ipconfig /all`. Windows 95/98 users can run the command `winipcfg`. Linux/UNIX users can type `ifconfig`.

Once you have determined the client's Ethernet address, click on the link to create a new hostname for a *local* host. Add the hostname of the target system, the Ethernet address along with the desired IP address into the web panel. From this point on specified IP address will only be provided to a client system with the matching Ethernet address.

11.6. E-mail Retrieval

As shown below, this section of the server manager allows you to specify the protocol used to retrieve e-mail from your ISP and configure other settings regarding the retrieval of e-mail.

Change e-mail retrieval settings

The e-mail retrieval mode can be set to **standard** (for dedicated Internet connections), **ETRN** (recommended for dialup connections), or **multi-drop** (for dialup connections if ETRN is not supported by your Internet provider).

E-mail retrieval mode:

Standard ☐

Your Mitel Networks server includes a complete, full-featured e-mail server. However, if for some reason you wish to delegate e-mail processing to another system, specify the IP address of the delegate system here. For normal operation, leave this field blank.

Delegate mail server:

For ETRN or multi-drop, specify the hostname or IP address of your secondary mail server. (If using the standard e-mail setup, this field can be left blank.)

Secondary mail server:

For ETRN or multi-drop, you can control how frequently this Mitel Networks server contacts your secondary e-mail server to fetch e-mail. More frequent connections mean that you receive your e-mail more quickly, but also cause Internet requests to be sent more often, possibly increasing your phone and Internet charges.

During office hours (8:00 AM to 6:00 PM) on weekdays:

Every 5 minutes ☐

Outside office hours (8:00 AM to 6:00 PM) on weekdays:

Every 30 minutes ☐

During the weekend:

Not at all ☐

For multi-drop e-mail, specify the POP user account and password. (If using standard or ETRN e-mail, these fields can be blank.) Also, for multi-drop, you can either use the default Mitel Networks server mail sorting method, or you can specify a particular message header to use for mail sorting.

POP user account (for multi-drop):

POP user password (for multi-drop):

Your choice of e-mail retrieval mode will depend on the arrangements you made with your Internet service provider:

- **If you have a dedicated connection**, set E-mail retrieval mode to "Standard".
- **If you arranged "ETRN" support with your ISP**, choose that setting and then scroll down to the field that asks for the IP address or hostname of your ISP's secondary mail server. This secondary mail server will provide temporary e-mail storage when your server is not connected to the Internet.
- **If you arranged "multidrop" mail service from your ISP**, choose "multidrop" and then scroll down to the field that asks for the IP address or hostname of your ISP's secondary mail server. This secondary mail server will receive all e-mail for your domain and store it in a single POP

will periodically fetch this mail and distribute it to individual POP mailboxes on the server. (Note that due to problems receiving mail for mailing lists, we *strongly* encourage people to *NOT* use multi-drop e-mail.)

- **If you are a ServiceLink subscriber**, choose "Guaranteed e-mail" in order to activate the guaranteed e-mail services.

If you want to forward e-mail to another mail server for processing, enter the mail server IP address in the box marked **Delegate mail server**. A common use for this is if your server is receiving inbound e-mail from the Internet, but you would like to pass that mail to a different mail server on your internal network.

If you have a dialup connection, the server allows you to control how frequently it fetches e-mail from your ISP. This is particularly useful in situations where you incur phone or Internet charges each time your system contacts your ISP. The default settings are every 15 minutes during standard office hours and every hour outside normal office hours on weekdays or on weekends. The fields allow you to customize those settings.

Finally, if you have "multidrop" mail service you need to select the sort method used by the server to decide which user each message should be delivered to. Your server has a default method for this (it examines various headers such as "To" and "Resent-To") which works in most circumstances but is not suitable for certain purposes such as mailing list messages. Some ISPs add a header to each e-mail message which can help your server determine the correct recipient. If your ISP does not add a header to multidrop e-mail, select the "Default" sort method and ignore the "select sort header" field. If your ISP does add a header to multidrop e-mail, then select "Specify below" and enter the header tag provided by your ISP. Because you *will* experience problems with mailing-lists when using multi-drop e-mail, we strongly recommend that you work with your ISP to have a special header added to each message. The "Default" sort method should be only used as a last resort.

11.7. Other E-mail Settings

This screen presents you with additional options for controlling how your system handles e-mail.

Change other e-mail settings

Administrative notices generated by the Mitel Networks server are normally e-mailed to the **admin** account. If you would like them to be e-mailed elsewhere, please enter the e-mail address below. Otherwise, leave this field blank.

Forwarding address for administrative notices:

Whenever the Mitel Networks server receives a message to an unknown user, it can be returned to the sender with an error message (recommended practice) or sent to your system administrator (as an administrative notice).

E-mail to unknown users:

Return to sender ☐

The Mitel Networks server can deliver outgoing messages directly to their destination (recommended in most cases) or can deliver them via your Internet provider's SMTP server (recommended if you have an unreliable Internet connection or are using a residential Internet service). If using your Internet provider's SMTP server, specify its hostname or IP address below. Otherwise leave this field blank.

Internet provider's SMTP server:

You can control access to your POP and IMAP servers. The private setting allows access only from your local network(s), and the public setting allows access from anywhere on the Internet.

POP and IMAP server access:

Private ☐

You can enable or disable webmail on this system. Webmail allows users to access their mail through a regular web browser by pointing the browser to www.tofu-dog.com/webmail, and logging in to their account.

Enable/Disable Webmail:

Disabled ☐

Save

- **Forwarding address for administrative notices:** The default address for administrative notices (i.e. undeliverable mail, backup notifications and other status/error messages) is "admin". If you'd like those messages to be sent elsewhere, enter the address here.

Note: Be aware that all messages sent to `postmaster`, `root` or `mailer-daemon` at your domain are sent to either `admin` or the address that you enter in this field.

- **E-mail to unknown users:** This field allows you to choose whether incoming messages to unknown users are bounced back to the sender or forwarded to the system administrator. Some users prefer the latter setting because it allows them to catch and reroute e-mail that was incorrectly addressed.

Note: If you choose to have messages forwarded to the system administrator, they will be sent to either "admin" or the e-mail address specified in the forwarding address field mentioned above.

- **Internet provider's SMTP server:** Normally the server will send outgoing messages directly to their intended destination. If, however, you have an unreliable connection or are using a residential Internet service, it may be advisable to route e-mail via your provider's SMTP server. In that case, you should enter the SMTP server's hostname or IP address here.

In fact, if you have a temporary dial-up connection to the Internet, you may find that you *need* to use your ISP's mail server in order to deliver mail to some locations. As a reaction to the huge volume of unsolicited commercial e-mail ("spam"), many Internet sites are refusing direct SMTP connections from IP addresses that are known to be temporary dial-up accounts. For this reason, you may need to use your ISP's mail server since it will have a permanent connection to the Internet.

- **POP and IMAP server access:** The options are "Private" and "Public". The former allows access only from your local network. The latter allows access from anywhere on the Internet. Think about this carefully. On the positive side, choosing "Public" access allows any of your users to retrieve their e-mail via POP/IMAP from anywhere on the Internet. The negative side is that when you do this, you are reducing your level of security, as you will now have two more services (POP and IMAP) that are listening for connections across the Internet. Both protocols also involve transmitting your password across the Internet in plain, unencrypted text, opening up the possibility that someone could intercept the packets and learn your username and password. Allowing such access can be a great convenience to your users, but if security is a concern you should consider using encrypted webmail instead.

IMPORTANT: Even with POP and IMAP configured for public access, users outside your local network are not able to *send* e-mail using your server as their SMTP host. Allowing this would open your server to abuse by spammers as a mail relay. Users who are travelling should either: a) use the SMTP server of their local ISP; b) use PPTP to connect to your internal network; or c) use webmail to read their mail. Webmail provides your users with secure access to both read and send mail via your server.

- **Enable/Disable Webmail:** With this option you can enable or disable the webmail component of your server. More information can be found in the Webmail chapter.

11.8. Review Configuration

This section of the server manager summarizes how your server is configured. This is the data that you entered during the installation process and possibly changed later through the server console or the server manager. As you can see from the screen below, this is essentially a report that you can print out for your records. You do not have the ability to make changes from this screen.

Review configuration

This report summarizes the networking, server, and domain parameters on this Mitel Networks server relevant to configuring the client computers on your network. You may wish to print this page and use it as a reference.

Networking parameters	
Server Mode	servergateway
Local IP address / subnet mask	192.168.202.1/255.255.255.0
External IP address / subnet mask	192.168.16.222/255.255.255.0
Gateway	192.168.16.1
Additional local networks	No additional local networks defined
DHCP server	disabled
Server names	
DNS server	192.168.202.1
Web server	www.tofu-dog.com
Proxy server	proxy.tofu-dog.com:3128
FTP server	ftp.tofu-dog.com
SMTP, POP, and IMAP mail servers	mail.tofu-dog.com
Domain information	
Primary domain	tofu-dog.com
Virtual domains	No virtual domains defined
Primary web site	http://www.tofu-dog.com/
Mitel Networks SME Server manager	http://ottawa1/server-manager/
Mitel Networks SME Server user password panel	http://ottawa1/user-password/
E-mail addresses	useraccount@tofu-dog.com firstname.lastname@tofu-dog.com firstname_lastname@tofu-dog.com

Chapter 12. Collaboration

12.1. User Accounts

User accounts should be set up for each person in your organization. A user account includes separate, password-protected e-mail and file storage areas.

If this is the first time you are setting up user accounts for your organization, you will need to establish what your naming convention will be. Let's assume you've decided that the account name should consist of first initial and last name. So, if you have an employee named Fred Frog, Fred's user account would be "ffrog". Assuming your domain name is tofu-dog.com, Fred's e-mail address would be "ffrog@tofu-dog.com". Fred's file directory on the server would also be named "ffrog". There are some basic rules built into the server as to what constitutes a valid account name. The account name must contain only lower-case letters and numbers and should start with a lower-case letter (not a number).

User account names are limited to twelve characters to maintain consistency with various versions of Windows. Longer names can be created for e-mail through the Pseudonyms panel. For your information, pseudonyms of "firstname.lastname" and "firstname_lastname" are automatically created for each account.

Create, remove, or change user accounts

[Click here](#) to create a user account.

You can modify, lock or remove any account or reset the account's password by clicking on the corresponding command next to the account.

If the account is marked as locked, that means that the user's password needs to be reset. Please note that newly created accounts are automatically locked until the password is changed.

Current List of User Accounts

Account	User Name				
ffrog	Fred Frog	Modify...	Reset password...	Lock Account...	Remove...
<i>ssalmon</i>	<i>Sally Salmon</i>	Modify...	Reset password...	<i>Account is locked</i>	Remove...

In the "User Accounts" section of the server manager, you will see a list of your current accounts. If you haven't already created any accounts, select "Click here" and fill in the requested information - the account name (the part of the e-mail address that comes before "@"), the person's name, address, department, company and phone number. As a convenience, the defaults that you entered in the "Directory" section of the server manager appear each time you create a new account. You can, if necessary, modify the information for each user as you create the account.

From the list of user accounts, you can easily modify or remove a user account (by clicking on "modify" or "remove" next to the user name) or set the user's password. **User accounts are locked out and cannot be used until you set the initial password for each account.** As a reminder of this, user accounts appear in red until the password is changed. (In the example shown here, the administrator has not yet changed the password for user "Sally Salmon").

Note: If you want someone to have an e-mail address at your company, but want the messages forwarded to another external e-mail address, you can create the user account but set the e-mail delivery option in the user account to *Forward to address below* and enter the external address. If you leave the user account locked out, the user will not be able to access services on your server, but the e-mail *will* be delivered to the external e-mail address.

12.1.1. Disabling User Accounts

There may be times when you do not wish to delete a user account but instead merely want to disable it. For instance, when an employee leaves the company, you may want to immediately remove their access to the server, but still keep their files or e-mail address active until the information can be examined. To disable any user account on your server, just click on the *Lock Account* link on the User Accounts web panel. *As soon as you click the link*, the account will be locked out. The user will no longer be able to retrieve e-mail or connect to any files or other resources on the server.

When an account is disabled, e-mail *will* still be received for that user name, but the user will be unable to retrieve the e-mail. As noted above, if a user account is set to forward e-mail to an external e-mail address, the e-mail *will* be forwarded to that external address. To prevent this, you will need to modify the properties for that user account.

To re-enable the user account, you need to reset the password using the link on the User Accounts web panel.

12.1.2. Changing User Passwords

Once they have an active account, your users can set their own passwords by accessing the user-password URL. They do this through their web browsers by visiting the URL **www.yourdomain.xxx/user-password** (where "www.yourdomain.xxx" is the web server name you entered into the server console). The staff at The Pagan Vegan would visit the URL **www.tofu-dog.com/user-password**.

To make the change, a user would enter his or her account name (the characters before "@"), the old password and the new password (to ensure accuracy, the screen asks for the new password twice). Note that changing the password for a user in the server manager overrides any previous password entered by your user. Therefore, when a user forgets his password, simply reset it in the server manager.

Note: There is no way for the administrator to recover a forgotten password for a user. All they can do is set a *new* password for the user.

12.2. Quota Management

By default, there is no size limit on the files a user may store on the server or the amount of e-mail he or she may receive. However, if you wish to limit the disk space a particular user account can use, you may do so on the "*Quota management*" panel in the server manager. As shown in the image below, you will see a list of user accounts, the actual disk space they are using and the quotas, if any, set for that user account.

Manage user account quotas

You can set filesystem quotas for users on your system by clicking the "Modify" button next to the user you wish to update.

If the user exceeds the "Limit with grace period", warnings will be generated. If this limit is exceeded for longer than a week or if the "Absolute limit" is reached, the user will be unable to store any more files or receive any more e-mail.

A setting of '0' for either limit disables that limit for the corresponding user.

The disk space for each user includes the user's home directory, e-mail, and any files in information bays which are owned by the user.

Current Quota Usage and Settings

Account	User Name	Limit with grace period (mb)	Absolute limit (mb)	Current usage (mb)	
ffrog	Fred Frog	0	0	46.85	Modify...
ssalmon	Sally Salmon	0	0	0.03	Modify...

Warning

Note that the quotas apply to **all** files that a user stores on the server. This includes not just their home directory, but also all files that they may put into any of the i-bays.

There are two quotas that can be applied to each user account:

- **Limit with grace period** - when a user's disk usage exceeds this limit, an e-mail warning message will be sent to the user account each night until the disk usage is brought back under the limit.
- **Absolute limit** - when a user's disk usage hits this limit, the user will no longer be able to save files to the server or receive e-mail.

Note that if the user account exceeds the "Limit with grace period" for seven consecutive days, the account will be treated as if it exceeded the absolute limit and will no longer be able to save files or receive e-mail.

Important: E-mail for the user account is **not** lost! It is held in the delivery queue and will be delivered to the user when their disk usage drops back below their absolute limit (or the "limit with grace period" if they were locked out due to seven days above that limit).

By selecting "*Modify...*" you are able to set a quota (in Megabytes) for a particular user account. Note that you do not have to set *both* limits for a user account and can choose to set only one of the limits.

If you set a limit and later wish to *disable* the quota for a given user account, all you need to do is set the limit to "0".

12.3. Groups

This screen allows you to create, remove or change user groups, which are simply lists of people with a shared interest - for example, they work in the same department or are collaborating on a project. The user group function serves two purposes in the SME Server V5 with ServiceLink: it permits e-mail to be sent conveniently to a group of users, and it allows the system administrator to associate groups of users with a single information bay (i-bay).

Creating a new group is a simple three-step process. You enter the group name (as with account names, these should begin with a lower-case letter and consist only of lower-case letters and numbers), followed by a brief description. Finally, check the boxes next to the names of the users who should be associated with that group.

Warning

When you create a group, you are required to assign *at least one* user to that group. If you fail to do so, the group will not be created and you will receive an error message.

After you add (or remove) a user account from a group, the user must log out and log back in for those changes to take effect. Until the user does so, he or she will still have their old group membership information. For instance, say that you create a new group "sales" and assign user "ffrog" (Fred Frog) to that group. You then create a new i-bay called "salesinfo" that only the "sales" group can access. Fred Frog is still logged into a Windows PC and now tries to connect to the new i-bay through Windows Explorer. He will receive a permission-denied error. He must log out of windows (he does not need to shut down or reboot, just log out) and login again. Now he should be able to go through Windows Explorer and access the "salesinfo" i-bay without any problem.

12.4. Pseudonyms

Any user who has an account on your SME Server V5 with ServiceLink will be able to receive e-mail sent to that user ID. For instance, if you have a user named Fred Frog with the user account "ffrog", his primary e-mail address will be "ffrog@mycompany.xxx".

Likewise, when you create a group account, that group account name functions as an e-mail *alias*, so that messages addressed to the group ID will be sent to all members of the group. If, for example, you create a group called "sales", messages to "sales@mycompany.xxx" will be distributed automatically to all members of that group. As you add and remove members to the group, your server automatically updates the e-mail alias.

In addition to user and group accounts, however, your server also automatically creates several *pseudonyms* . For instance, for *each* user account, the server creates two separate pseudonyms using the first and last names of the user. These two pseudonyms are in the form of "firstname.lastname" and "firstname_lastname". Hence, when you create the user account "ffrog" for a user with the name Fred Frog, he will also be able to receive e-mail sent to "fred.frog@mycompany.xxx" and "fred_frog@mycompany.xxx".

Additionally, your server creates a special pseudonym called "everyone" that includes all user accounts on the system. Two other pseudonyms, "postmaster" and "mailer-daemon" are created pointing to the "admin" user.

If you wish to modify or remove any of these pseudonyms, or create new ones, you can use the web panel found under the "Collaboration" section, as shown below.

Note: The special pseudonyms of "everyone", "postmaster" and "mailer-daemon" will only be visible after you have either added a user account to the system or have added a custom pseudonym. Until that time, these three pseudonyms are there, but will not be visible on the Pseudonyms web panel.

Create, remove or modify pseudonyms

[Click here](#) to create a pseudonym.

The Mitel Networks Server automatically creates an e-mail alias for each group. If you want to define an e-mail alias for a list of users, simply create a group and the list will automatically be maintained by the server.

Pseudonyms allow you to create other names for existing users or groups. For example, you may wish to create a pseudonym "webmaster" for your "webdevelopers" group or a pseudonym "joe" for the user "joseph".

The server automatically creates pseudonyms of the form firstname.lastname and firstname_lastname for every user on the system and a pseudonym "everyone" which contains all users on the system.

You can modify or remove a pseudonym by clicking on the corresponding command next to the pseudonym.

Current List of Pseudonyms

Pseudonym	User or group		
everyone	Everyone (local network only)		
mailer-daemon	Administrator		
postmaster	Administrator		
fred.frog	ffrog	Modify...	Remove...
fred_frog	ffrog	Modify...	Remove...
sally.salmon	ssalmon	Modify...	Remove...
sally_salmon	ssalmon	Modify...	Remove...

As noted on the screen below, there are some restrictions on the text content of the names. Pseudonyms can be linked to existing user or group accounts. In the example shown, a pseudonym for *webmaster* is being set to point to *ffrog*.

Create a pseudonym

Pseudonyms should contain only lower-case letters, numbers, period, hyphen and underscore and should start with a lower-case letter or number. For example "sales", "john.holland", "123" and "email-administrator" are all valid pseudonyms, but "John Smith" and "Henry Miller" are not.

Pseudonym name:

Select account or group:

12.5. Information Bays

The i-bay (information bay) feature of the SME Server V5 with ServiceLink is a simple, very flexible and powerful way for you to share information with others. It is a rich enough feature that we've devoted an entire upcoming chapter to discussing i-bays.

12.6. Virtual Domains

When you are supporting multiple domains on a single server, each domain being served is referred to as a *virtual domain*. (The strict definition of virtual domain is when a single IP address is shared between multiple domains.) When you create a virtual domain using this section of the server manager, your SME Server V5 with ServiceLink will be able to receive e-mail for that domain and will be able to host a web site for that domain.

To create a virtual domain, fill in the domain name and a description of the site. You then tell the server where to find the content for that domain - it can be the same as your primary web site, or you can create a new set of web pages and store them in one of your i-bays. Clicking the arrow in the "Content" field will show you a list of your current i-bays and allow you to make a selection. This feature allows you to host multiple web sites from a single server.

Be aware that you can point the virtual domain to either the *primary* web site or to one of the *i-bays*. You cannot point a virtual domain to a subdirectory that you simply create inside of the primary web site file area. You need to use an i-bay instead.

Note: When you are entering the name for the virtual domain, you should supply the *fully-qualified domain name*. This is the full name of the domain, including any extensions like ".com", but *without* any prefixes like "www" or "ftp". For instance, you can create a virtual domain by entering "tofu-bird.com", but *not* by entering "tofu-bird" or "www.tofu-bird.com".

Once you have created a virtual domain, your server will be automatically configured to answer to web requests for *www.domainname.xxx* and will accept e-mail for your virtual domain as well.

Important: While the server is prepared to offer web and e-mail services for this virtual domain, there is one more step that must occur. In order for users on the Internet to successfully connect to your machine using the virtual domain, you will need to work with your ISP or whoever controls the DNS entries for your virtual domain to have the appropriate DNS entries pointed to the IP address of your server. For instance, your ISP will need to configure an MX record for the domain in order for you to receive inbound e-mail to that domain. ServiceLink subscribers will have this automatically taken care of as part of their ServiceLink subscription.

Chapter 13. ServiceLink

Until you sign up for ServiceLink and your server is registered, all of the panels in this section of the server manager will not be functional. In order to subscribe to ServiceLink, visit <http://www.mitel.com/> (<http://www.mitel.com/>) and find a authorized reseller near you.

The Mitel Networks Corporation authorized reseller will interact with the Mitel Networks NOC (Network Operations Center) to obtain a Service Account ID for your server. Once that number is entered into the Status panel on your server, you will be subscribed to ServiceLink. Your authorized reseller will enable ServiceLink services and they will begin to function. Once subscribed, your server will synchronize at a periodic interval (the default is one hour) with our NOC to retrieve updated information such as virus pattern files.

Be aware that one of the features of our NOC is that alerts can be established to notify your authorized reseller (or any e-mail address they set) when your server has missed a sync period, when e-mail is arriving at the NOC instead of your server, and when viruses have been detected. You will also be able to receive monthly reports from your authorized reseller detailing ServiceLink activity.

13.1. Status

Until ServiceLink is activated, the Status panel will appear as shown in the image below.

ServiceLink Activation

In addition to the standard features of this server software, you can now take advantage of Mitel Networks ServiceLink, an integrated suite of network-delivered services that enhance the security, reliability and functionality of your Mitel Networks SME Server. ServiceLink delivers critical system-management services including 24 x 7 monitoring and status reports, virus protection with automatic updates, point-and-click IPSEC Virtual Private Networks, guaranteed e-mail delivery and DNS services.

To read more about the benefits of Mitel Networks ServiceLink, please visit <http://www.e-smith.com/serviceLink/>

To activate ServiceLink, you will require a service account ID which can be obtained from your Mitel Networks SME Server Authorized Partner. If you have already obtained a service account ID, please enter that ID now.

Service account ID:

As mentioned above, you will need to arrange with a Mitel Networks Corporation authorized reseller to subscribe to ServiceLink. Once you are subscribed, the Status page will change to show your current status. As shown in the image below, this panel also allows you to manually initiate a synchronization with the Mitel Networks NOC.

ServiceLink Status Information

This web panel is used to provide updated ServiceLink status information for this Mitel Networks SME Server. Status information is downloaded from the Network Operations Center (NOC) to the server as part of the synchronization protocol.

The display includes information about your ServiceLink account, the latest synchronization event status, and a list of services available from ServiceLink for which this server is subscribed. The display also includes the expiration date for each subscribed service and, if applicable, any error notice for that service. Click on the notice for more detailed information.

If you wish to deactivate your ServiceLink account, please click [here](#).

Your service account ID is **3946922**.

Your descriptive server name is **"Ottawa Office"**.

The last sync completed successfully at **Fri Nov 23 07:44:14 2001**.

Current ServiceLink subscription listing

Service	Status	Expires	Messages
DNS services	Subscribed	2002-11-23	None
Guaranteed e-mail	Subscribed	2002-11-23	None
Server support	Subscribed	2002-11-23	None
Virus protection	Subscribed	2002-11-23	None
IPSEC VPN service	Subscribed	2002-11-23	None

If there is an issue with any of your services, it will appear in red italics and you can follow a link to determine the problem. Note also that the expiration of your ServiceLink subscription appears.

13.2. Virus Protection

As soon as you are subscribed to ServiceLink and the Virus Protection service is enabled, all of your inbound and outbound mail messages will be scanned for viruses. The scanning software checks both the message body as well as all attachments.

If a virus is found on a message, the message is quarantined in a special mail folder and notifications are sent out about the virus. For an inbound message, the recipient at your site, the original sender and your Mitel authorized reseller are notified. For an outbound message, only the sender (at your location) and your authorized reseller are notified.

In the server manager the configuration screen shown below allows you to enable or disable e-mail virus scanning. You also have the option of enabling the scanning of all files in home directories or i-bays.

ServiceLink Virus Protection

The ServiceLink Virus Protection service is available. This service can scan all incoming and outgoing e-mail messages for your Mitel Networks server, including webmail. It can also scan home directories, and information bays. Which components should be enabled?

- ☐ Scan e-mail
- ☐ Scan home directories
- ☐ Scan information bays

To view the quarantined messages, we recommend you login to webmail as the "admin" user. You will be then able to view the messages without any code being executed. (**Do not open the attachments as doing so can infect your system.**)

Note: Administrators with Linux experience can also use ssh to the server and login as the "root" user to use the command-line mail programs `mutt` or `pine` to view the messages.

Scanning of home directories and i-bays is *disabled* by default and must be specifically enabled on the server. Once enabled, the server will scan the designated areas once each night. When an infected file is detected, an e-mail message is sent to the administrator. If the authorized reseller has configured the NOC to send them alerts when viruses are detected, they will also be notified.

Warning

While the administrator and possibly authorized reseller are notified that an infected file has been detected, the file is *not* disinfected automatically and will need to be cleaned by the administrator.

Each time your server syncs with the NOC, it will check to see if a new virus pattern file is available. If a new file exists, it will be downloaded and installed automatically. All e-mail and file virus scanning will start using the file immediately.

13.3. DNS Services

During the ServiceLink subscription process, your server will be enabled to publish DNS records through our NOC. As shown below, this panel in the server manager reports which domains you are publishing under the header "*DNS Services*".

Note: With ServiceLink you are able to publish domains in the top-level domains of `.com`, `.org` and `.net`. Other top-level domains may be possible for an additional charge. Note also that ServiceLink includes the publication of two domains. More than two domains can be published for an additional charge. Contact your authorized reseller for more details on either of these issues.

ServiceLink DNS services

DNS services configuration

You can change your service domain at any time. The change will be reflected following the next synchronization with the Network Operations Center. Note that this operation will completely remove your previous service domain, including any hosts that you have already configured.

.e-smith.net

Update

DNS hosting

The following is a list of domains on your system and those which are being published as part of your DNS subscription to Mitel Networks SME Server with ServiceLink:

Domain	Status	Comments
tofu-dog.com	Domain has not been requested for publishing.	
tofu-dog.e-smith.net	Domain has been accepted for publishing.	

With ServiceLink, changes you make in the Hostnames and addresses panel of the server manager will automatically be published to the global Internet. A checkbox is available for each hostname that asks " Publish globally?". If you check that box, the record will be transferred to the NOC and from there published out to the larger Internet.

If, as shown in the screen above, there are domains that indicate they are not currently being published, your authorized reseller can use the NOC to configure those domains to start publishing your information. Be aware that it may require several business days for some domains to be registered and published.

The top part of the panel allows you to configure a *service domain* that is available to you after ServiceLink activation. This domain takes the form of *yourdomain.e-smith.net* and allows you to immediately start receiving e-mail and connecting to your server using that domain.

If you wish to change the service domain name, you can do so using this panel by entering your new name and clicking the *Update* button. If the domain you want is not available, you will be notified and will be able to choose another name. Service domain changes take effect immediatly after the next synchronization with the NOC.

Warning

The change of service domain takes place upon the next synchronization of your server with the NOC and your previous service domain will be *completely removed*. This includes entries for any hosts that you may have been publishing for the previous service domain.

Mitel Networks Corporation does not guarantee the availability of a domain name and reserves the right to refuse to register any domain name. All ServiceLink users publishing DNS domains must adhere to regulations and rules provided by ICANN and our registrar.

13.4. IPSEC VPNs

Through the Partner Zone interface to our NOC, your Mitel Networks Corporation authorized reseller is able to very simply and easily create a secure IPSEC VPN between your server and other ServiceLink-enabled servers. This provides an economical way of creating a private network between different offices without having to pay for expensive VPN equipment of dedicated connections. Each location just needs a connection to the Internet and a ServiceLink-enabled server. A VPN can be established between just two offices, or between a wide number of offices. All communication occurs using the extremely secure IPSEC protocol, so no one can intercept and read your data as it travels across the Internet.

Note: IPSEC VPNs can only be established between servers operating in *server-and-gateway mode*. If you have a server operating in *server-only mode*, it will not be able to participate in an IPSEC VPN.

Once your authorized reseller has established a VPN, the web panel (shown below) will show that your server is a member of a VPN and provide information about the other systems to which your server is connected.

ServiceLink IPSEC VPN

The ServiceLink IPSEC VPN service allows one to configure a virtual private network between sites over the internet using a secure protocol. When two or more Mitel Networks servers with ServiceLink IPSEC VPN are configured into a VPN, those servers are then able to share files as if each is a machine on the local network.

Your service account id is **3946922**.

Current list of VPN partners

Description	System name	External IP	Local network	status
Chicago Office	osprey.lodestar2.dyndns.org	24.43.204.34	192.168.24.0/24	enabled

From a user perspective, the major difference will be that when you open up (on Windows) your "Network Neighborhood" or "My Network Places", you will now see the servers at the other locations on your VPN.

Note that when you establish a VPN using ServiceLink, one SME Server is designated to act as the "primary" server. All user accounts are created on this primary server and users must login with those accounts to access network resources. The other servers in the VPN (known as secondary servers) will function as gateways for the users on their local networks to access the VPN and Internet.

Chapter 14. Administration

14.1. Blades

Blades are a feature in SME Server V5 with ServiceLink which allow you to easily install or remove software modules via the server manager. Using this feature will allow easy customization of your server. You can choose the options required for your particular needs without having to add unnecessary features.

Warning

Be aware that the installation of certain blades may void your support agreement. Before installing any blade, we strongly suggest you consult with your authorized reseller.

If you have not registered for ServiceLink, you will see a list of default blades that are available to be installed. If, however, you have chosen to subscribe to ServiceLink, your server will display a regularly updated list of available blades, which can be installed simply by clicking on the *Install* link next to the desired item in the server manager.

Blades are developed and made available by Mitel Networks Corporation or by the open source developer community and are split into categories. "Supported" blades have been verified by our development staff and ServiceLink subscribers will be able to obtain support for the installation and configuration of those blades. "Unsupported" blades are typically those contributed by the open source community and for which no technical support is directly available from Mitel Networks Corporation.

Clicking on "Blades" in the server manager's navigation menu will show a list of available software blades which can be installed on your system. When you click on the "Install..." link, you will be able to view the license for the blade and complete the installation.

When blades are installed, many of them will create a new panel in the server manager that allows you to configure the blade. However, some contributed blades may not be configurable through the server manager and may require use of the Linux command prompt. Again, please note that installing unsupported blades may void your support agreement.

Note that outside of blades, you can still customize your server using Linux utilities from the command prompt (if your support agreement permits such customization). However, blades provides a much simpler and easier way to perform this customization.

14.2. Backup or Restore

You can easily back up the contents of your SME Server V5 with ServiceLink using one of two methods. Both are controlled through the web panel shown below.

Backup or restore server data

The Mitel Networks SME Server provides two ways to back up and restore your server: using your local desktop or a tape drive.

The first method creates a copy of your server configuration and user data files, and downloads it to your local desktop via your web browser. Currently your configuration and data files total approximately **79Mb**. The "Verify desktop backup file" option can be used to check the integrity of a desktop backup file.

The tape backup method uses a software package called *flexbackup* to back up your entire hard disk to tape every night. This requires a supported tape drive and a tape that is not write-protected. The backup is performed automatically at the selected time every night (with a reminder automatically e-mailed to the administrator during the day). Currently your hard disk contains **426Mb** of data.

Both restore methods allow you to restore your configuration and user data files. **Ideally, the restore should be performed on a freshly installed Mitel Networks SME Server.**

Backup configuration and status

Tape backups are **disabled**.

Select an action:

You have four actions you can perform, each of which is described in the following sections.

14.2.1. Backup To Desktop

The first type of backup allows you to save a snapshot of your server configuration onto your desktop computer. This will save all user accounts, user directories, i-bay contents and web content, as well as the configuration parameters entered using the server console and the server manager. The web panel shows you the size of the backup file so that you can verify whether sufficient space exists on your desktop machine.

When you choose **Backup to desktop**, a browser window will appear that will allow you to name the file and select the location on your desktop where the file will be saved.

14.2.2. Restore From Desktop

If you ever need to restore the original configuration and files to your server, simply select **Restore from desktop** and a browser window will prompt you to select the backup file from your desktop. Restoration of the information is automatic.

Warning

Ideally you should use **Restore from desktop** on a freshly installed server. Therefore, if you are planning to do a restore, you should first re-install the SME Server V5 with ServiceLink software and *then* perform the "Restore from desktop" command.

14.2.3. Verify Desktop Backup File

This option allows you to verify that the backup to disk was completed successfully. In rare cases we have found that users ran out of disk space on their client PC while doing the backup to desktop. This options allows you to verify whether or not the backup did in fact complete successfully.

14.2.4. Configure Tape Backup

The second type of backup involves configuring your system to perform a daily full system backup to a tape drive using a software package called *flexbackup*. If you wish to activate this option, check the box next to **Enable Tape Backup** and then specify the time at which you wish the backup to occur and the time at which reminder notices should be sent.

Enable/Disable Nightly Tape Backup

Select whether you wish to enable nightly backups. Then indicate the desired times for the backup and the load tape reminder.

The tape backup requires a supported tape drive. A warning message will be sent to the administrator at the designated reminder time if the tape drive is empty.

Enable tape
backup ☐

Tape backup time of day (hour/min)	<input type="text" value="12"/>	<input type="text" value="00"/>	AM/PM: <input type="text" value="AM"/>
Load tape reminder time of day (hour/min)	<input type="text" value="12"/>	<input type="text" value="00"/>	AM/PM: <input type="text" value="PM"/>
<input type="button" value="Update Configuration"/>			

Be aware that you must use a supported tape drive and that a tape must be inserted in the drive for the backup to work.

Note: Reminder e-mail messages for tape backups are automatically sent to the e-mail address that is configured to receive administrative notices. This is normally the user *admin*, but you can change this by going to the Other e-mail settings screen in the server manager.

14.2.5. Restore From Tape

If you are performing regular backups, you can also restore user data and configuration settings by using the **Restore From Tape** option. After you press the *Perform* button, the system will read the files from tape and overwrite any currently existing files. **You must reboot your system** after the restore for the changes to take effect. Note that in order to restore data from tape, you must have first checked off **Enable Tape Backup** and scheduled nightly backups. If you have not done this, you will not be able to restore from tape using the server manager.

Warning

Note that this restore procedure *only* restores user data and configuration information. It does *not* restore system files. If you experienced a serious system crash, you should *first* re-install the SME Server V5 with ServiceLink software and then perform a restore from tape.

14.3. Reinstallation Disk

Using this section of the server manager, you can create a reinstallation diskette which will aid in the recovery process in the unlikely event that you encounter a system failure and are required to reinstall the software. The reinstallation diskette will record system and network configuration data for your current system so that you will not need to re-enter that information when you reinstall.

Warning

Each time you alter your system configuration, you **MUST** make a new reinstallation disk (or overwrite your old one). Otherwise, your existing reinstallation disk will not contain your updated configuration data - which means that after reinstalling the software, you will not automatically see your most recent data.

Note: Be aware that when you are performing this task, the diskette must be in the **server** diskette drive, *NOT* the diskette drive of your local desktop computer.

Note that this reinstallation disk serves a *different* purpose than the "emergency boot disk" you created as part of the original software installation process. The emergency boot disk allows you to boot your server if you are unable to boot from the hard disk for some reason. For instance, this could occur due to a hardware error or through a mis-configuration of the LILO boot loader during an advanced customization procedure. The emergency boot diskette does not change your software or make any other adjustments to your system.

The reinstallation disk, on the other hand, will boot your system directly into the *software installation process* and will completely reinstall the SME Server V5 with ServiceLink software. It will, however, save you the steps of entering all the network configuration data and allow you to simply move through the configuration screens using the "Keep" option.

14.4. Mail Log File Analysis

If you are using your SME Server V5 with ServiceLink to send and receive e-mail, there are now a number of reports available that can help you analyze your system's performance. While the default setting provides basic statistics, if you pop up the menu, you will see a range of other options. If you suspect that there is a problem with the delivery of your e-mail, you can use these reports to see how your system is operating. The information can also help you decide how best to optimize your system.

14.5. View Log Files

This panel allows you to view the system log files on your server. As shown in the image below, you select the log file that you want to view and press the "View Log File" button. Without any filter options, you will see the entire log file.

View Log Files

This panel allows you to view the log files generated by the services running on your Mitel Networks server.

Choose a log file to view:

You may optionally specify a filter pattern to display only the lines from the log file which match this pattern. If you leave this field blank, all available lines of the log file will be displayed.

Filter Pattern (optional):

You may also optionally specify a highlight pattern to mark in bold any lines from the log file which match the highlight pattern. The highlight pattern is applied to any lines which have already matched the filter pattern.

Highlight Pattern (optional):

Please note that it may take quite some time to generate these reports.

[View Log file](#)

You will probably find the log file of most interest to be `messages` where most of the system services write log messages. If you enter any text in the "Filter Pattern" box, only lines of the log file containing that text will be displayed. If you enter any text in the "Highlight Pattern" box, that text will be shown in bold. Both options can be used together. Be aware that the filter is case-sensitive.

As an example, if you were interested in messages relating to DHCP, you could examine the log file `messages` with a filter pattern of `DHCP`. This will show you all DHCP-related messages. If you further add a highlight pattern of `DHCPACK`, the messages relating to DHCP acknowledgements will appear in bold.

14.6. Reboot or Shutdown

If you need to shut down or reboot your server, using this screen will ensure that the shutdown sequence occurs gracefully, preserving all configuration and information on your server. There is a similar function in the server console as well. Note that this screen initiates the shutdown or reboot **immediately** after you click the "Perform" button.

Chapter 15. Miscellaneous

15.1. Online manual

This link will take you directly from the server manager to the online user guide available at <http://www.e-smith.org/docs/manual/> (<http://www.e-smith.org/docs/manual/>). Note that you must be connected to the Internet to read the online user guide.

15.2. Create Starter Web Site

If you already have a customized web site, you should not use this section, since it will overwrite your `index.htm` file.

If you do not have a customized web site and wish to create your starter home page, simply fill out the appropriate fields. This will create a basic home page that you can visit by entering your domain name for your site, `http://www.yourdomain.xxx`, in your web browser. Note that, as previously explained, there is typically a delay of one or more days before your ISP publishes your domain address records. On your local network, you can use "`http://www/`" to view your starter web site.

At any point in the future, you can replace or revise your starter web page by replacing or revising the files in the `html` directory on your server. The `html` directory for your web site can be accessed using Windows file sharing. Ensure you are logged onto your network using the `admin` name and password and then use file sharing to go to the server. Select the "`primary`" share and then select the "`html`" directory.

15.3. Other Administration Notes

Accessing administrative areas of your server via Windows file sharing: To access administrative areas of your server using Windows file sharing, you must be logged into your network as "`admin`" with the server system password. This applies particularly to the `NETLOGON` share (where you can edit the `netlogon.bat` file), the *Primary* share (where the main web site is stored) and any i-bays that are writable only by the user *admin*.

Chapter 16. Information Bays (i-bays)

Information bays, or i-bays, are a unique feature built into your SME Server V5 with ServiceLink. i-bays are a powerful, simple, flexible mechanism for creating distinct information-sharing sites. The network administrator can define several characteristics for each new i-bay they create:

- **write access:** the administrator can control access to the i-bay by associating the i-bay with a group. All groups previously created in the groups section of the server manager will appear in the drop-down menu under "group" in this section. In addition, two default groups will always appear - "administrator" and "everyone" (meaning all users, whether on the local network or on the Internet).
- **user access via file-sharing or FTP:** The administrator can also control who has the ability to save a file into or modify the contents of the files in the i-bay (write access) and who has the ability to view the contents of the i-bay (read access). The administrator can specify whether the entire group can write to the i-bay or whether the administrator alone has the power to save files to the i-bay. Similarly, the administrator can control whether group members only can read the contents of the i-bay or whether the contents can be read by anyone.
- **password protection:** the administrator can specify whether a password is required to access an i-bay from the Internet and what that password will be.

Note: If you select *Password Required*, users who connect to the i-bay via FTP or HTTP will be prompted to supply that particular i-bay's username and password. The *user* name is always the name of the i-bay and the *password* is whatever the administrator assigns to that i-bay - not the individual user's password. Note that, as with user accounts, i-bay accounts are locked out by default. *If* a password is required, users will not be able to access the i-bay until the administrator sets the password.

i-bays are simple to create and manage. The "Information bays" section of the server manager shows all current i-bays, the name of each i-bay and a description of its contents. In this section, you can delete an i-bay (which will delete all contents of the i-bay directory) and, if the i-bay requires a password, you can set it here. As with your user account directory, any i-bay that requires a password will appear in red until that password has been changed from "default" (the i-bay for Samson's Farms in the following image is an example of this).

A note about i-bay names: When you create an i-bay, the name may be up to 12 characters long¹ and may contain only lower-case letters, numbers, periods and underscores. The i-bay name should also start with a lower-case letter. For example, `johnson`, `sales` and `client3.prj8` are all valid names, while `3associates`, `John Smith` and `Bus-Partner` are not. Finally, an i-bay cannot use the same name as an existing user or group account. It must be unique. Note that there are two special names, *primary* and *public*, which are in use by the system and cannot be used for an i-bay name.

Create, remove, or change information bays

[Click here](#) to create a new information bay.

You can remove any information bay or reset its password by clicking on the corresponding command next to the information bay. If the information bay shows up in red, that means that the password has not yet been changed from the default, and should be changed soon.

Current List of Information Bays

Name	Description			
intranet	Pagan Vegan Intranet	Modify...	Reset password...	Remove...
menus	samples of menus invitations etc	Modify...	Reset password...	Remove...
mgabriel	Art Exposition by Miles Gabriel	Modify...	Reset password...	Remove...
<i>samfarms</i>	<i>Samson's Farms</i>	Modify...	Reset password...	Remove...
sharedfiles	Pagan Vegan shared files	Modify...	Reset password...	Remove...

16.1. i-bay Directories

Each i-bay has three directories - `html`, `files` and `cgi-bin`. Each directory is briefly outlined below:

- **cgi-bin:** This directory is set aside to hold "CGI scripts" used for that i-bay's web pages. CGI scripts are tools used in advanced web site creation and are not discussed here.
- **files:** This directory holds files that can be accessed either locally only or publicly. It can be used for such things as a company download site, a company-wide file sharing server, or a document sharing site for a specific customer. When someone connects to the i-bay using FTP, they will see the files in this directory.

1. This 12-character restriction ensures that the i-bay can be shared correctly to all Windows machines.

- **html:** When an i-bay is accessed using a web browser (via http), the user will enter the `html` directory and the web browser will automatically open the index file (usually `index.html` or `index.htm`) in that i-bay. In other words, it will display the web page associated with that i-bay. This means you can have different web sites running on your server, each associated with a specific i-bay. This can be very powerful and useful, as you will see in the upcoming examples.

Generally, you can think of the `html` directory as the place to put all files, images and documents that you would like to be accessible through the *web*. The `files` directory is for all files that you want people to access through FTP or regular file sharing. Note that you can have as many subdirectories as you wish underneath either `html` or `files` but you cannot create additional directories at the top level of the i-bay.

Note: If an i-bay is set for *no public access via web or anonymous ftp*, users connecting to the i-bay through Windows or Macintosh file sharing will see only the contents of the `files` directory. However, if the i-bay settings are later changed to *allow* public access through web or anonymous ftp, users will then see the top-level directory of the i-bay with the three subdirectories of `html`, `files` and `cgi-bin`. The items they were used to seeing before will now be found in the `files` directory.

16.2. Accessing the i-bays

You can access the contents of an i-bay using a web browser, Windows file sharing / AppleTalk, or FTP.

- **accessing an i-bay using a web browser (via http):** To view an i-bay using a browser, enter "`www.yourdomain.xxx/i-bayname`". For example, the URL for Samson's Farms i-bay is "`www.tofu-dog.com/samfarms`". Assuming you are entitled to access this i-bay, you will see the `index.html` page in the `html` directory in the Samson's Farms i-bay. If a password is required to see the contents of the i-bay, a password dialog box will appear before the contents of the i-bay are served to the web browser.
- **accessing an i-bay via Windows file sharing and AppleTalk:** To access the i-bay using Windows file sharing or AppleTalk, simply navigate to the server over your network browser (in Windows, this would be via "Network Neighborhood") and select the i-bay you want to enter from those appearing. You can only access an i-bay in this way if you are on the local network.
- **accessing an i-bay via the FTP server:** To access the i-bay using FTP, you use your FTP client to connect to your server and use the *i-bay name* as the login id. If the i-bay requires a password, you will need to enter the *i-bay password* as well. If you are using a command-line or graphical FTP client, you will usually be prompted for the login username and password. If you are using a web browser, you will need to enter a FTP URL. This will be in one of the following forms, depending on whether or not a password is required:

```
ftp://ibayname@ftp.domainname
ftp://ibayname:password@ftp.domainname
```

Warning

Be aware that FTP transmits all passwords in the clear **without encryption** and can therefore be a security risk. If you are concerned about security, we suggest you consider the `scp` "secure copy" command associated with `ssh` as an alternative to FTP.

Note that users accessing the i-bay via FTP in this manner are not able to *upload* files to the i-bay. They can only *download* files from the i-bay to their client.

It is possible to upload files using FTP, but to do so you must login to the server with a valid user name, *not* the i-bay name. That user account must be a member of the group that has been given write permission for the i-bay (configured on the i-bay screen). You would then change to the i-bay directory (using the `ftp` command "`cd ../ibays/ibayname`"). You will now be able to upload files from your FTP client to the appropriate directories.

In the next few sections, we will take a look at some examples of i-bays that have been created by our hypothetical catering and event-planning company, The Pagan Vegan, to demonstrate their capabilities.

16.3. Creating an i-bay

No matter how you are going to use an i-bay, the process of creating an i-bay starts by clicking on the "Click here" link at the top of the Information Bays panel in the server manager. You will be presented with the form shown in the image below.

Create a new information bay

The information bay name should contain only lower-case letters, numbers, periods, hyphens and underscores, and should start with a lower-case letter. For example "johnson", "intra", and "cust3.prj12" are all valid names, but "3associates", "John Smith" and "BusiPartner" are not.

Information bay name:

Brief description:

Group:

User access via file sharing or user ftp:

Public access via web or anonymous ftp:

Execution of dynamic content (CGI, PHP, SSI):

(*) The public access mode "password required outside local network" is not supported by the FTP server component. If you select this mode, the FTP server will require a password both inside and outside the local network for this i-bay.

You now need to fill out the form providing the information and making the choices described below. Note that the ftp access described below can be overridden by the **FTP access limits** setting on the Remote access panel of the server manager. If you choose to "Disable public FTP access" there, ftp access for individual i-bays will *not* be allowed, even though you *will* appear to be able to enable it from the i-bay configuration screen.

- **Information bay name:** This is the short name of the i-bay (subject to the 12-character length restriction mentioned earlier). The i-bay name will be what users will enter in the URL after the hostname to access the i-bay from the web. For instance, if public access is enabled, an i-bay named 'intranet' can be accessed by the Pagan Vegan staff at 'http://www.tofu-dog.com/intranet'.
- **Brief description:** This text will appear in various administrative screens and can be a useful reminder of the i-bay content.
- **Group:** Ownership of the i-bay content is assigned to an existing group. The group ownership plays a role in the next setting for user access.
- **User access:** You need to decide who will be able to add and modify content in the i-bay and who will be able to read the content.
- **Public access:** Here you set what type of public access you wish to have for the i-bay. If the i-bay is just to be used by a small group of users, you can leave public access set to the default of *None*. If you want others to be able to access the i-bay via web or anonymous ftp, you can choose to allow access to just the local network or the wider Internet. You also can choose whether or not you wish to require a password.

Note: If you choose one of the modes of *Public access via web or anonymous ftp* that requires a password, public access will not be available until you set the i-bay password from the main information bay panel in the server manager. Once you do so, users can access the i-bay through their web browser or ftp by using the *i-bay name* and *i-bay password*, rather than their own user name and password.

- **Execution of CGI scripts:** If you want to use CGI scripts to add functionality to your web site, you can execute those scripts from the `cgi-bin` directory of your i-bay. However, for security reasons you must first choose *enabled* here to allow such scripts to be executed.

Once done filling out the form, click the *Create* button and the server manager will create your i-bay. If you wish to change these settings at any later point, you can click on *Modify...* next to the i-bay name in the information bays panel of the server manager.

16.4. Modifying an i-bay

At any point in time you can modify the attributes of an i-bay (except for its name) by clicking on the "*Modify...*" link next to the i-bay name on the "Information bays" panel of the server manager. For instance, you can easily change the description, group ownership, and access methods.

There are, however, a few items to be aware of when modifying i-bays:

- If an i-bay is set for *no public access via web or anonymous ftp*, users connecting to the i-bay through Windows or Macintosh file sharing will see only the contents of the `files` directory. However, if the i-bay settings are later changed to *allow* public access through web or anonymous ftp, users connecting through file sharing will then see the top-level directory of the i-bay with the three subdirectories of `html`, `files` and `cgi-bin`. The items they were used to seeing before will now be found in the `files` directory. This may disrupt Windows shortcuts and configuration settings. (The good news is that simply changing the public access setting back to "None" will return i-bay file sharing access to its previous configuration.)

- After an i-bay is modified, all Macintosh users will be disconnected from the i-bay and will need to reconnect. All Macintosh users will receive an alert stating that they will be disconnected in 5 minutes.

Outside of those concerns, you can modify the i-bay as often as you wish. If you wish to change the actual *name* of the i-bay, you will need to remove the i-bay and create it again. (Note that this will delete the *contents* of the i-bay, so make sure you have backed up the i-bay data before you remove it.)

16.5. An i-bay Used as a Customer Site: The Miles Gabriel Art Exposition

"The Pagan Vegan" (TPV) has found that customers like having access to a customized web page which summarizes all of the information pertaining to their particular event. The company finds it reduces the risk of miscommunication and improves its image and reputation. The ".html" files in the i-bay's html directory are based on a template that TPV uses for each customer. Creating each web site is a straightforward, fill-in-the-blanks process.

Create a new information bay

The information bay name should contain only lower-case letters, numbers, periods, hyphens and underscores, and should start with a lower-case letter. For example "johnson", "intra", and "cust3.prj12" are all valid names, but "3associates", "John Smith" and "Bus!Partner" are not.

Information bay name:

Brief description:

Group:

User access via file sharing or user ftp:

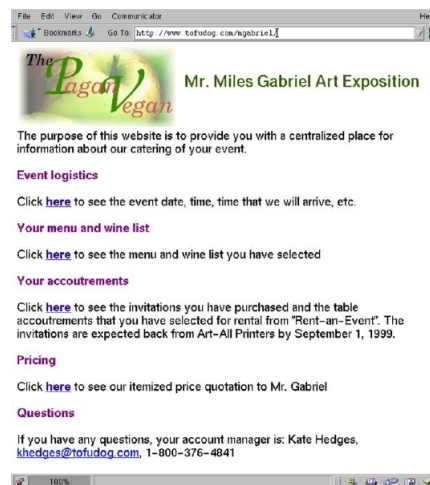
Public access via web or anonymous ftp:

Execution of dynamic content (CGI, PHP, SSL):

(*) The public access mode "password required outside local network" is not supported by the FTP server component. If you select this mode, the FTP server will require a password both inside and outside the local network for this i-bay.

Create

TPV has chosen a naming convention for i-bays that customers can easily remember - first initial, last name. Because it contains important customer information, only the site administrator can save files into this i-bay. To prevent others from accessing the customer's i-bay, a password is required to enter the site. (TPV created individual passwords and securely provided them to their customers.)



Miles Gabriel has contacted The Pagan Vegan to cater an art exposition. The Pagan Vegan has created an i-bay specifically for Mr. Gabriel's account called "mgabriel". Mr. Gabriel accesses the site with the URL **www.tofu-dog.com/mgabriel**. As you can see, Mr. Gabriel has access to a summary of his event information. He can check at any time to ensure the arrangements are correct. For example, at midnight tonight he can access his i-bay to show his spouse the design used for his invitations!

16.6. An i-bay Used as a Shared Network Drive

Having a shared network drive can be very helpful as a way of storing and sharing documents company-wide. TPV uses an i-bay for a

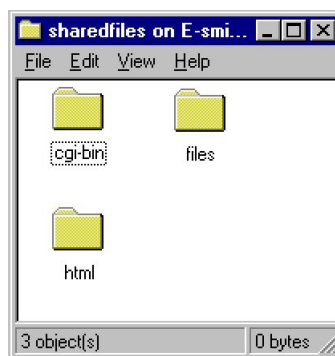
The i-bay is accessed via Windows file sharing, AppleTalk or FTP. To access using file sharing, simply access the server over the network (via Network Neighborhood) and open the appropriate i-bay. You will see the files located in the `files` directory and can then open them or copy them to your system.

Note: This is only true if the i-bay has been set to allow public access via web or anonymous ftp. If an i-bay is set for *no public access via web or anonymous ftp*, users connecting to the i-bay through Windows or Macintosh file sharing will simply see the *contents* of the `files` directory. However, if the i-bay settings are later changed to *allow* public access through web or anonymous ftp, users will then see the top-level directory of the i-bay with the three subdirectories of `html`, `files` and `cgi-bin`. The items they were used to seeing before will now be found in the `files` directory.

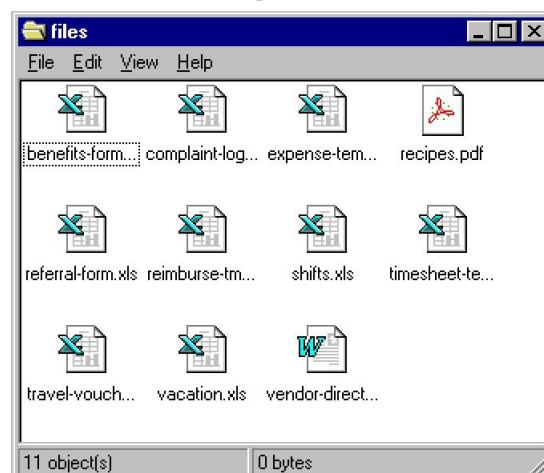
As an example, when the staff of The Pagan Vegan goes into their Network Neighborhood, they double-click on "E-smith-server" as shown in:



They will then see a list of i-bays accessible through Windows file sharing. When they click on one of them called "sharedfiles", they see the three folders inside of the i-bay:



When they go inside of `files`, they will then see the list of documents provided there:



As you can see in this example, The Pagan Vegan has several files in this directory for company use. Providing a centralized location for company documents (such as expense report templates) ensures that everyone always has access to these documents and uses the most up-to-date version.

16.7. An i-bay Used as an Intranet: The Pagan Vegan "Vegemite"

The Pagan Vegan has created an i-bay for its company newsletter / intranet. The company has found this to be a good way for employees to express themselves and share information.

Create a new information bay

The information bay name should contain only lower-case letters, numbers, periods, hyphens and underscores, and should start with a lower-case letter. For example "johnson", "intra", and "cust3.prj12" are all valid names, but "3associates", "John Smith" and "BusiPartner" are not.

Information bay name:

Brief description:

Group:

User access via file sharing or user ftp:

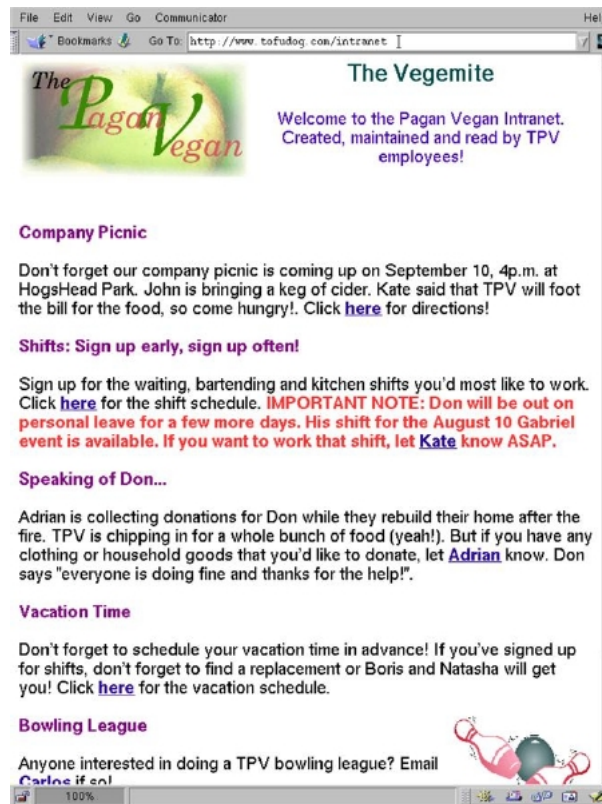
Public access via web or anonymous ftp:

Execution of dynamic content (CGI, PHP, SSL):

(*) The public access mode "password required outside local network" is not supported by the FTP server component. If you select this mode, the FTP server will require a password both inside and outside the local network for this i-bay.

In keeping with TPV's culture, the newsletter is very casual. The company has a high degree of trust in its employees, and, as a result, employees are given full access to the contents of the intranet so anyone on staff can revise it. A more typical company might want the intranet to be created by a particular staff member and "checked in" by the administrator (write access "administrator only").

The intranet is, of course, viewable only from the internal network. No password is required. To access the intranet, TPV employees use their web browsers to access the URL **www.tofu-dog.com/intranet**.



This particular newsletter was created using a desktop office application called StarOffice (similar to Microsoft Office). The files were created as typical word processing documents, saved into ".html" format and then transferred into the html directory of the "intranet" i-bay using Windows file sharing. Starting with just a blank document, it took only about an hour to create the main page and the other pages that make up this newsletter.

16.8. An i-bay Used to Expedite Processes: Samson's Farms

Samson's Organic Farms delivers fresh produce to The Pagan Vegan every week. Samson's and TPV use an i-bay to improve the ordering and delivery process. TPV has created an i-bay for Samson's called "samfarms". It is accessible to the external Internet but password-protected so that only staff at TPV and Samson's Farms can read it. Anyone on TPV's local network can write to it.

Create a new information bay

The information bay name should contain only lower-case letters, numbers, periods, hyphens and underscores, and should start with a lower-case letter. For example "johnson", "intra", and "cust3.prj12" are all valid names, but "3associates", "John Smith" and "BusiPartner" are not.

Information bay name:

Brief description:

Group:

User access via file sharing or user ftp:

Public access via web or anonymous ftp:

Execution of dynamic content (CGI, PHP, SSL):

(*) The public access mode "password required outside local network" is not supported by the FTP server component. If you select this mode, the FTP server will require a password both inside and outside the local network for this i-bay.

Here's how the process works:

- Each week, Mr. Samson updates his online order sheet to include only produce that will be ripe and ready for the next delivery date. He saves it in ".html" format and e-mails it to The Pagan Vegan's administrator.
- Upon receiving the e-mail, TPV's administrator saves the file directly into the html directory of the "samfarms" i-bay.
- The chef accesses the samfarms i-bay, reviews what produce will be available, and plans menus.
- The chef's assistant then reviews the menus, checks against existing inventory and determines what should be ordered. The assistant enters TPV's order directly onto the order sheet in the samfarms i-bay using an HTML editor.
- The day before delivery, the chef reviews his assistant's order (as shown in the image below) using a web browser and makes any last minute adjustments.

Vegetables		Fruit	
artichokes	8 /dozen	apples (Mac)	/peck
beans	10 /lb	black berries	4 /flat
beets	/lb	blue berries	6 /lb
broccoli	10 /lb	crab apples	2 /peck
carrots	20 /lb	grapes (black)	/lb
cauliflower	6 /lb	nectarines	2 /peck
celery	20 /lb	oranges (navel)	/peck
corn	6 /dozen	peaches	/peck
eggplant	6 /lb	pears (bosc)	2 /peck
endive	4 /lb	raspberries	4 /flat
fennel	4 /lb		
garlic	4 /lb	Herbs	by the bunch
leeks	/lb	basil (purple)	20

- On the day of delivery, Samson's shipping staff accesses the i-bay over the Internet, prints out TPV's order from the samfarms i-bay, and fills it.

16.9. An i-bay Used as Your Customer Download Site

When customers hire The Pagan Vegan to plan events, they need to review a great deal of information - menu options, catalogues from various vendors for event stationary, table-setting rentals, etc. Often customers want several days to review it all. TPV has only a limited number of catalogues for loan, so it decided to provide customers with access to this information online. To accomplish this, TPV created a download i-bay, called "menus", where customers can download the catalogue files themselves and view the contents on their desktop machines.

Create a new information bay

The information bay name should contain only lower-case letters, numbers, periods, hyphens and underscores, and should start with a lower-case letter. For example "johnson", "intra", and "cust3.prj12" are all valid names, but "3associates", "John Smith" and "BusiPartner" are not.

Information bay name:

Brief description:

Group:

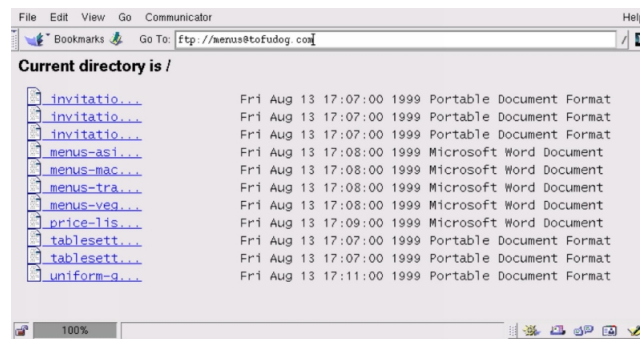
User access via file sharing or user ftp:

Public access via web or anonymous ftp:

Execution of dynamic content (CGI, PHP, SSL):

(*) The public access mode "password required outside local network" is not supported by the FTP server component. If you select this mode, the FTP server will require a password both inside and outside the local network for this i-bay.

TPV set the i-bay for Administrator-only write access, viewable over the entire Internet, with no password required. A customer accesses the site using the FTP client in their web browser to login as the i-bay user name by entering the URL **ftp://menus@ftp.tofu-dog.com**. This is what the customer sees:



When the cursor is placed over a file name, the full name of the file appears. To download a particular file, the customer simply clicks on the file name. A browser window allows the customer to select a destination directory for the file on his or her local hard drive.

Chapter 17. User File Storage on the SME Server V5 with ServiceLink

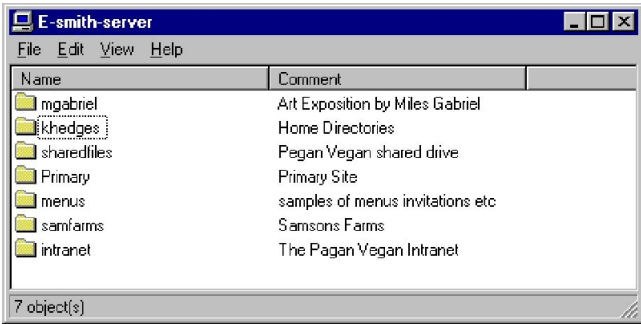
When you create a user account on your server, this not only creates an e-mail account but also a file directory for that user. This directory is set aside for files that the user would like to store on the server hard drive. It can only be accessed by the user. To access the directory, the user would navigate to the server via Windows file sharing or AppleTalk.

17.1. Windows

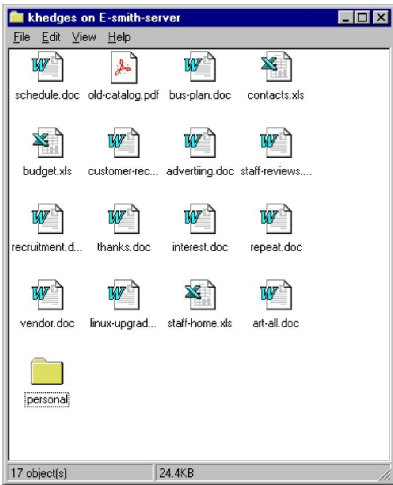
For example, in Windows the user would open "Network Neighborhood". In the Network directory, you will see all machines accessible to you on your network. The server should be one of them. If it isn't viewable, you may not be logged onto your network under the correct name/password (see the section below on this) or your machine may not be in the same workgroup as the server.



When you click on the server, you will see all i-bays and directories available to you. You will also see the Primary directory (which houses the company web page information). In the example below, Kate Hedges is logged onto her local network as khedges (her account name) with her correct password. When she enters the server, she can see all the i-bays (mgabriel, samfarms, sharedfiles, menus and intranet), as well as her own user directory.



By clicking on her own user directory, "khedges", she can see all of the work and personal files she has chosen to store on the server, as shown in the image below.



Note that for users who are on a Windows network, the user must be logged onto the network with the name and password associated with the server user account.

To do so, open the "Start" menu.

- Select "Shut down".
- Select "Close all programs and log in as a new user".
- Enter the username (in our example, above, it would be "khedges")
- Enter the current password for that user on the server.

If you change the password on your server, you must also change the password for "admin" on your PC. To do this:

- Use the File Manager to search for the file "admin.pwl".
- Delete this file and simply log into Windows networking as above.

17.2. Macintosh OS

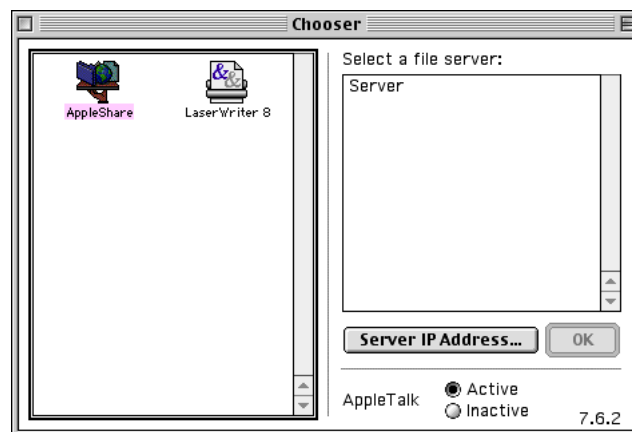
To use file sharing from a Macintosh computer, you will need to be set up to use AppleTalk over Ethernet, and to communicate using TCP/IP over Ethernet.

The first step is to choose your Ethernet adapter (usually "Built-in Ethernet" or just "Ethernet") from the AppleTalk Control Panel. If everything is plugged in correctly, the panel should quickly say that no zones were found. If this takes a while, the network cable or network card may not be working properly, and you should see an Apple technician.

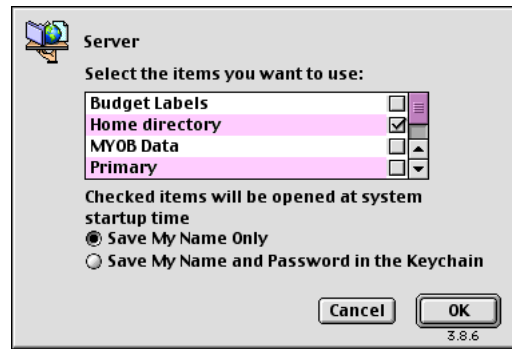
To use AppleTalk over TCP/IP it is best that your Mac's network settings are configured via DHCP. The server provides this service, but it must be enabled via the server manager. To enable it on your Mac, choose "DHCP Server" in the TCP/IP control panel. If the control panel asks for a Client ID, simply type in any unique title, such as "Design G4" or "Reception".

Note: AppleTalk will work without TCP/IP, but will be slower than AppleTalk over TCP/IP.

The next step is to choose a server to connect to via AppleTalk. Click on the Chooser icon in your Apple Menu to bring up a list of file servers to connect to.



Double clicking on the server will bring up a list of all the volumes available for you to connect to, whether or not you have sufficient privileges to use them. Your screen should now look like the following picture.



The "Primary" volume is your default area set up by your server for sharing files and the company web site, while "Home directory" points to the specific user's own space on the server, viewable only by that user. While other i-bays may appear, you may not be able to use them, as you must be a member of the group owning that i-bay to use it.

The highlighted volumes are those you wish to connect to. Any ticked volumes will attempt to mount every time you boot your Mac. If you wish to save passwords in a keychain (Mac OS 9.0 or above), you should read the tutorial available from the help menu on your Mac.

Once you have chosen your volumes to mount, whether or not they are ticked, a dialog box will appear to allow you to log in.



Use your server user name and password to connect. This screen will pop up only once, as the information typed in will be used for every subsequent login. This includes clicking on the Chooser, your server, and then other volumes to mount them as well.

Your desktop should now have icons for each successful volume, such as the icons below:



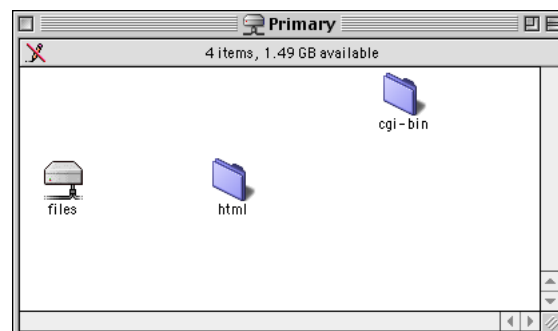
MacOS 8.5 or above



MacOS 7.5 to 8.1

Notice the wire at the bottom of the icon, denoting a network volume.

Clicking on one of these icons should show you a window similar to the one below. While you should not be able to add files or folders to this window, you may do so in the files, html or cgi-bin folders (permissions allowing).



Note: Some programs may not work well if run from the server. Programs such as MYOB (multi-user accounting software) rely on certain specific nuances to share the same file with multiple other Macs. Test your applications with multiple users before relying on them in this situation.

Chapter 18. Webmail

If you wish, you can configure your SME Server V5 with ServiceLink so that users can access their e-mail via a web interface. Once webmail is enabled, users will be able to access their e-mail from the local network or anywhere in the world via the Internet using any standard web browser (provided it supports Javascript and tables, which almost all browsers do).

For added security, the server supports the use of *Secure Socket Layer (SSL)* connections. When your users connect using SSL, all communication between their browser and your web server is securely encrypted to prevent eavesdropping.

Note: The specific program we use for webmail is the *Internet Messaging Program (IMP)*. If you would like more information about IMP, you can visit the project web site at: <http://www.horde.org/imp/>

If you intend to enable webmail, you should consider whether your users will use webmail exclusively or will use webmail part of the time (for example, when travelling) and a regular e-mail client the rest of the time. If they plan to use webmail and another client, they should make sure that the other client uses the IMAP protocol. If they use POP3, their e-mail messages will be pulled down from the server into their local e-mail client and will therefore not be visible when the user logs into webmail. If IMAP is enabled on the local client, the messages will remain on the server and will be visible both from the local client and via webmail. (For more information on IMAP and POP3, read the earlier section in Chapter 7.)

A second issue is that using webmail *will* affect the performance of your server. We recommend that you evaluate your server hardware if you plan to use webmail. (Note that webmail can always be *disabled* later if you find that your system is not performing well.)

18.1. Enabling Webmail On Your System

Because the use of webmail can be resource-intensive, the server ships with webmail *disabled* by default. To enable the use of webmail, perform the following steps:

1. Connect to the server manager and login as the admin user.
2. Click on Other e-mail settings and scroll down to the section where you have the option to *Enable/Disable Webmail*. You now have two options:
 - **Enabled (secure HTTPS access only)** - Allows users to connect *only* through a secure SSL connection. This is **strongly** recommended because a regular HTTP connection transmits your mail account password across the network (or Internet) in plain, unencrypted text.
 - **Enabled (HTTP or HTTPS)** - Allows your users to connect through a secure or an insecure web connection.

After you perform these steps, your users should be able to connect and use webmail.

18.2. Starting Webmail

To use webmail, a user first needs a valid user account and password on your server. Next, the user opens up a web browser and points it to your server using an address resembling the following URL:

```
https://www.tofu-dog.com/webmail/
```

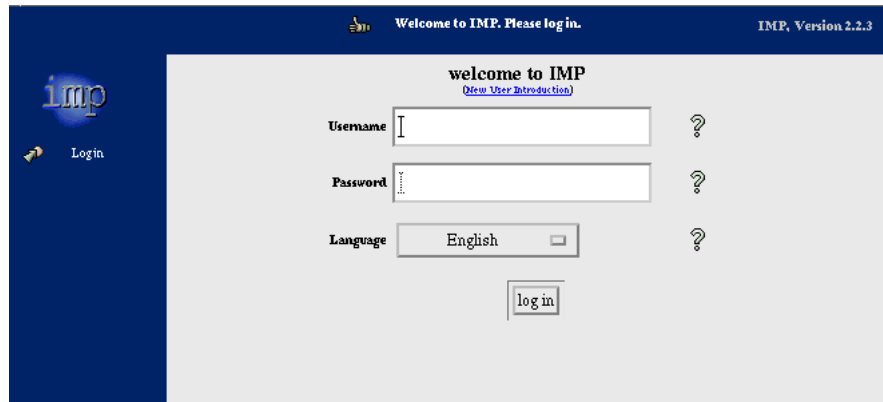
The **https** in the URL indicates this connection uses SSL encryption and provides a secure communication session.

Note: The exact address used in the URL will depend on how you have configured your server. In the example above, *www.tofu-dog.com* points to the server located at The Pagan Vegan and *https* indicates that they are using secure communication using SSL encryption. If you choose to provide insecure access, which we do *not* recommend, the URL would begin with *http* instead of *https*. You will need to provide your users with whatever URL will get them to your server.

Note that if your server is behind another firewall, that firewall will need to allow traffic through on TCP port 443 in order for SSL connections to take place.

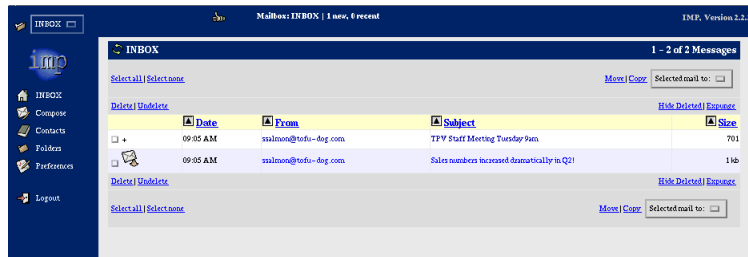
18.3. Logging In

Once connected, a user will immediately be confronted with a login screen similar to that shown in the screen below. From this screen you can read the help menu (by clicking on the link for *New User Introduction* at the top of the page) or login with your normal network user ID and password. Note that IMP supports a wide variety of languages for users for whom English is not their native language. (Or who have some desire to have menus in a different language!)



18.4. Viewing The Inbox

Once logged in, you will see your inbox, as shown in screen below.



Let's take a quick tour of the Inbox window.

In the top left corner is a pop-up menu that shows the list of your available mail folders. In your first webmail session, the only folder choice will be *INBOX*. As soon as you send an e-mail message, a folder called *sent-mail* will be created and available in the menu. You can also create additional mail folders at any time.

In the top center portion of the window is a status message indicating the folder you are in and the number of new or recent messages in that folder.

On the left side is a navigation menu allowing you to compose new messages, modify contacts, create folders, modify preferences or logout of the webmail system.

In the main part of the window are the actual messages. Each message has an icon denoting its status at the far left, the date/time of the message, who it is from, the subject and the size. Messages may be sorted by clicking on the column heading. You can read a message simply by clicking on the subject or sender of a specific message. The envelope/arrow icon that you can see in the status area of the second message in the image above indicates that this message is new.

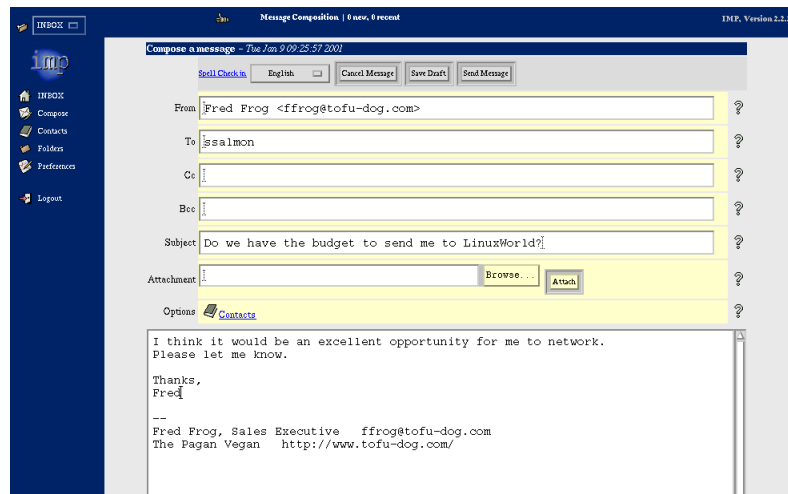
We will describe the various functions in greater detail later in this chapter, but this should be enough to get you started.

18.5. Logging Out of Webmail

Before we discuss the features of webmail, it is important to emphasize that you must **always** click on the *Logout* menu item when you are finished using webmail. If you do *not* do so, anyone else who uses your web browser on your computer (until you exit your web browser or logout of/shutdown your computer) will be able to read your messages and send messages from your account. After a successful logout, you will see the webmail login screen with a message at the top of the screen indicating that your logout was successful.

18.6. Composing Messages

To compose a new message, click on *Compose* in the menu on the left. You should see a screen similar to that below.



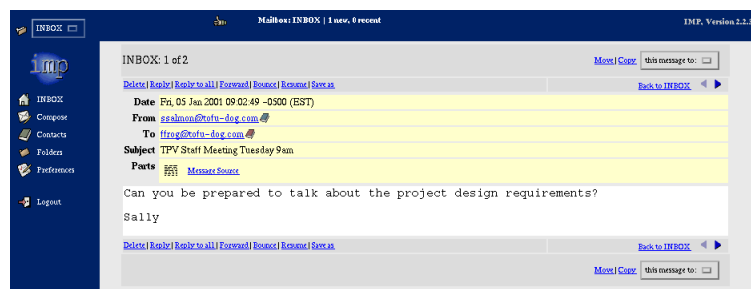
At the top of the compose screen, your available options include the ability to spell-check the message in your language of choice, or to cancel, save a draft or send the message.

If you choose to save a draft, your message will be saved in a folder called *drafts*. You may later retrieve this message by using the popup menu in the upper left corner to switch to the "drafts" folder.

Below that are the familiar e-mail fields for you to fill out. At the bottom of the page, the menu of commands is repeated for your convenience.

18.7. Reading Messages

To read a message, click on the *From* or *Subject* fields of the message. You should see a screen similar to the one below.

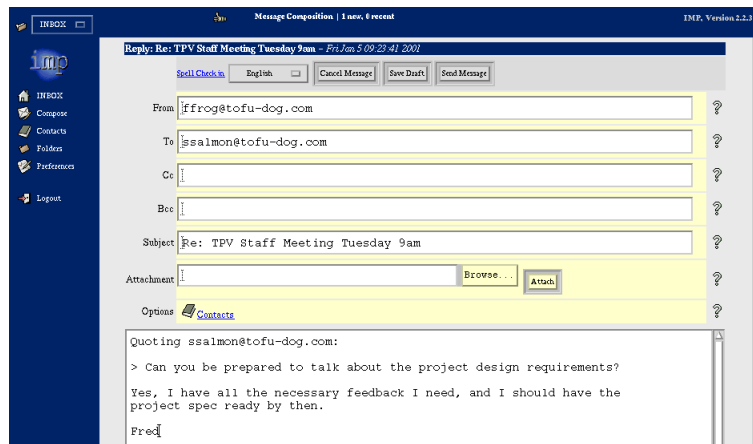


You now have several options. You can:

- **Delete** the message.
- **Reply** only to the sender.
- **Reply to all** of the original recipients.
- **Forward** the message to someone else.
- **Bounce** the message to another person (similar to "Forward" but without providing you the opportunity to comment).¹
- **Save As** - save the message to a text file.

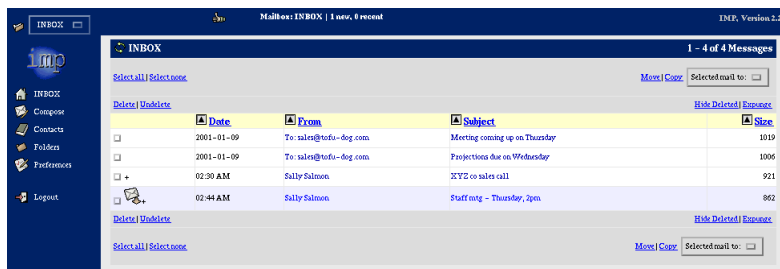
By clicking on the *Reply* button, you will be able to enter a reply window such as that shown below. Notice that the original message text is "quoted" with a ">" character in front of it. At this point, you can type more text or edit existing text, add or delete recipients, spell-check the message and do anything else that you could do in a normal compose window. Again, you can choose to cancel the message, save a draft or send the message.

1. In fact, the bounce command will send the message on to a third-party without indicating that you were the one forwarding it. So if "ffrog" sent a message to the "sales" group (of which you are a member) and you then bounced it to another user, that user would see the message coming from "ffrog" and going to "sales", but *your* name would not appear anywhere in the visible headers. Compare that to a "forward" command where the recipient knows you are the person forwarding the message.



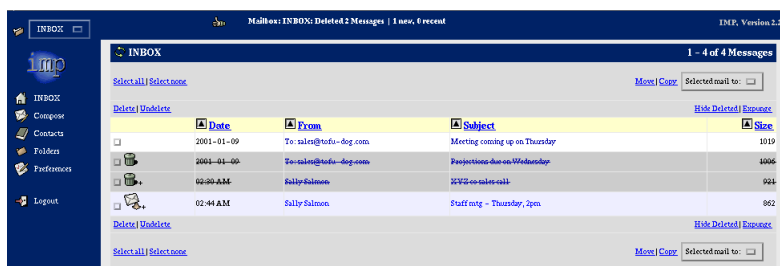
18.8. Deleting Messages

You can delete a message while reading it, as mentioned previously, or you can delete a message - or a group of messages - from the Inbox view.



To do so, check the box next to each message you wish to delete. After that, press the *Delete* text button directly above or below the list of messages on the left side. You will now see a trash icon next to the checkbox and a line through the messages.

As an example, in the image above, our user (ffrog) wants to delete the second and third messages. He can click on the checkbox next to each message and then click *Delete*. This will produce a screen such as that below.

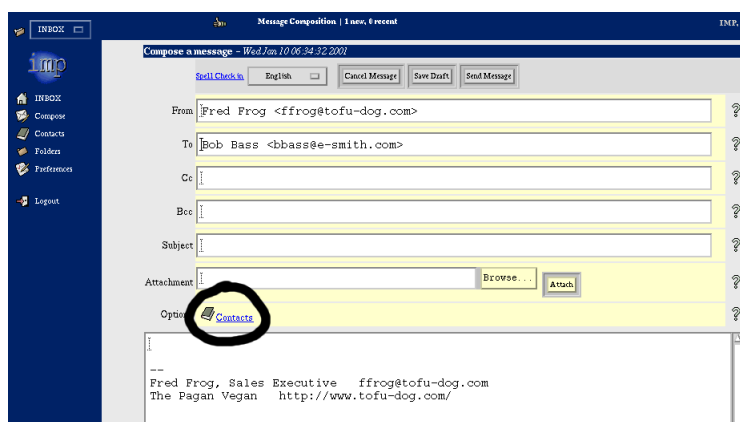


If you do not want to see the deleted messages, you have two choices. If you click on the **Hide Deleted** text button on the right side, the messages will be hidden from view, but will still be there and could be recovered with the *Undelete* button. If you choose **Expunge**, the messages will be permanently deleted.

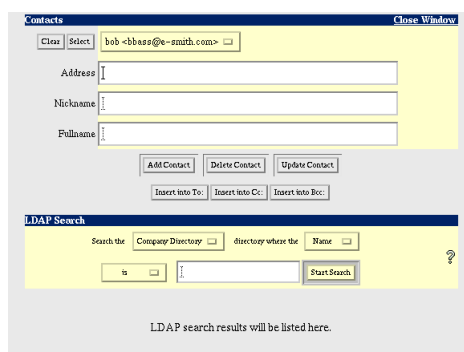
18.9. Using Contacts

The server webmail system provides two means of keeping track of e-mail addresses. First, you can have your own *Contacts* list. Second, you can easily access the company directory that lists all users and groups that have been created.

You can view and edit your contacts through two menu choices. From the left menu you can choose *Contacts*. This allows you to view or edit contacts, but does *not* allow you to add a contact to an e-mail list. To add a contact, you must open the Contacts window from the "Contacts" link in a Compose window, as highlighted in the image below.



In either case, you will find yourself viewing a window that looks like the one below.



If this is the first time you have entered the Contacts window, you will not see anything next to the "Select" button. Normally, though, you will see a pop-up menu with all of your contacts in it (as seen in the window above where "bob <bbass@e-smith.com>" appears). To enter a new contact, simply type the e-mail address, a "nickname" that will appear in the Contacts list, and the full name of the person. You must fill out all three fields. Then click *Add Contact*.

To update a contact's information, select the user's name/address from the contacts pop-up menu. The information should automatically appear in the fields. (If it does not, after selecting the entry from the pop-up menu, press the *Select* button next to the menu.) Enter the new information and click *Update Contact*. In a similar fashion you can delete a contact by selecting the contact from the pop-up menu and pressing the *Delete Contact* button.

As mentioned earlier, if you entered the Contacts window from the link in the Compose window, the three buttons - *Insert into To:*, *Insert into Cc:*, and *Insert into Bcc:* - will allow you to transfer the contact information directly into the Compose window.

To search the company directory, use the lower section of the Contacts window labeled *LDAP Search*². You have the ability to search either the entire name field or just the surname. Enter the text you are searching for in the entry box and choose how you want to compare the text against the directory. The default is to search for entries where the name **is** the text you enter, which requires an exact match. You may find it more useful to search for entries where the name **contains** the search text. A search with "contains" will find names where the search text appears *somewhere* in the name.

After entering your text and choosing your search options, press the *Start Search* button to query the directory. As shown in the screen below, your results will be returned in a new *LDAP Results* section of the same Contacts window. As with the section at the top of the screen, you choose your entry from the pop-up menu (or press the *Select* button if your entry is displayed already) and the information should appear in the entry box below. Assuming you entered Contacts from the link in the Compose window, you can now insert this information into the To, Cc or Bcc lines of the Compose window.

Note that you also have the option of inserting this entry directly into your Contacts list. If you have a large company directory, you may find this a useful way of ensuring that frequently used contacts are readily available.

Note: Unlike your local Contacts list, you cannot directly update entries that are in the company directory. Instead, those entries must be updated by the system administrator using the *Directory* panel in the server manager. See the *Directory* section of Chapter 11 for more information.

2. The search is called an *LDAP search* because the directory is queried using the *Lightweight Directory Access Protocol (LDAP)*, one of the most common protocols used on the Internet for searching directories.

18.10. Changing Webmail Preferences

By clicking on the *Preferences* link on the navigation menu, you can modify preferences for your webmail session, as shown in the screen below.

You have four preferences you can configure:

- **Signature** - You may include any text that you wish to appear by default at the bottom of your e-mail messages. Once configured, it will *always* appear at the bottom of a Compose or Reply window when you enter that window. You can, however, delete it for a specific message simply by editing the text in the Compose or Reply text window.
- **Full Name** - If you leave this blank, all of your messages will appear to recipients as having come from your e-mail address. If you enter text here, recipients will usually see that text first instead of your e-mail address.
- **From Address** - By default your From address is your regular system e-mail. **You do not need to set it here.** Enter an address here only if you want people to see a different reply address than your normal system-generated e-mail address.
- **Preferred Language** - This allows you to specify the language used in the menus.

When you are done modifying your preferences, press the *Save Preferences* button at the bottom of the page.

Chapter 19. Additional Software

In the process of developing the SME Server V5 with ServiceLink, we found it necessary to include some additional open source software. While Mitel Networks Corporation does not provide direct technical support for this additional software, its availability on the server may be of benefit to advanced users.

Warning

Use of this software is at your own risk and should not be attempted unless you know what you are doing! Mitel Networks Corporation does NOT provide support for this software.

MySQL

MySQL is a free, open source database management system. It provides a fully functional relational database similar to that provided by many commercial database vendors. We use it here as the back-end for our webmail application. More information about MySQL can be obtained at <http://www.mysql.com/>.

PHP

PHP is a web scripting language that has become popular because it easily allows developers to create dynamically generated web pages. Additionally, it includes commands that allow for easy interaction with databases, particularly MySQL. The PHP language resembles C or perl and is actually embedded in the actual HTML pages on the web server. If you are familiar with Microsoft's Active Server Pages, PHP works in a similar manner. We have installed it on the server because it is needed as part of our webmail application. To learn how to use PHP in your own web pages, please read the PHP FAQ at <http://www.php.net/FAQ.php> (<http://www.php.net/FAQ.php>) and the manual at <http://www.php.net/manual/> (<http://www.php.net/manual/>).

Procmail

procmail is an open source mail processing tool that can run on the server to preprocess incoming mail messages perform actions such as filtering them into folders. More information about procmail can be found at: <http://www.procmail.org/>. Additionally, members of our developer community have contributed HOWTO documents that show how to use procmail on our server. See <http://www.e-smith.org/docs/howto/> for links to those documents.

Taper

taper is a open source tape backup program provided for those who wish an alternative to the *flexbackup* program used by default in the server manager. More information about taper can be found at: <http://www.e-survey.net.au/taper/>.

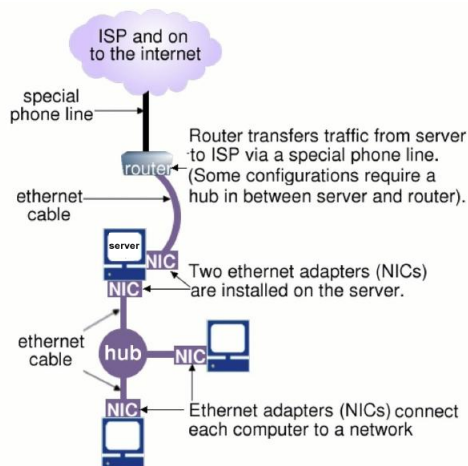
Appendix A. Introduction to the Ethernet Local Area Network (LAN)

A local area network (LAN) is the system of wires and other hardware that connects the computers within your office and allows them to communicate with one another. An ethernet LAN is the most common type. Ethernet refers both to a kind of connection and to a protocol for how Internet data packets travel around your network.

The **hub**, a common component of an ethernet, serves as a point of interface between computers on the network. Each computer on your network is connected to the hub using an ethernet network cable. Different hubs operate at different speeds: slower hubs, operating at 10 MB/sec, are suitable for small networks; faster hubs, operating at 100 MB/sec, are suitable for larger networks. Switching 10/100 MB hubs can operate at either speed, and provide a good way to upgrade your network gradually.

An **ethernet adapter**, also called an ethernet card or network interface card (NIC), connects each computer to the ethernet LAN. An server with a dedicated Internet connection requires two ethernet adapters; one connects it to your LAN and the other connects it to the external network that leads to your ISP. If your server connects to your ISP using a modem or ISDN adapter, it only requires one ethernet adapter.

A **router** ensures that Internet data packets (e.g. e-mail, web page information, etc.) reach the appropriate computers on your network. Routing is one of the functions performed by the server in server and gateway mode.



Allowing a third party, such as a systems integrator or networking company, to install your ethernet can be a good idea. It can help you select, procure and install the appropriate ethernet adapters, hub and cables. There are also various how-to guides available in bookstores if you are committed to installing it on your own.

Appendix B. Dynamic DNS Services

Tip: ServiceLink subscribers do not need to worry about a dynamic DNS service as DNS service is provided as part of the base ServiceLink subscription.

If your IP address is assigned dynamically, you may find it helpful to use a dynamic DNS service. A dynamic DNS service provides you with an automated way to notify them whenever your IP address changes so that they can immediately publish new DNS records for your domain. Without dynamic DNS, you would have to contact your ISP to have them change your DNS records, and your web site and other services would be unavailable for several days until the change was processed. You can easily enable the usage of a dynamic DNS service by selecting it on your server console.

A dynamic DNS service can be a great solution when used with a dedicated connection. With a typical dialup connection, your IP address changes much more frequently (possibly every time your server connects) and, because the server only connects intermittently, there is a delay in informing the dynamic DNS service of the change. This means that the risk of misdirected information is much greater with a dialup connection. For this reason, we recommend and support the use of dynamic DNS services only for dedicated connections.

Mitel Networks Corporation has tested four dynamic DNS services, of which two are free services and two are commercial services: yi.org (free), dyndns.com (commercial), tzo.com (commercial) and dyndns.org (free). For simplicity, we have preprogrammed the server to work with these services (including pre-installing their client software). If you have arranged dynamic IP address assignment from your ISP and you wish to use one of these services, all you need to do is visit the appropriate web site to sign up for service, and enable that particular function in the server console. In pre-configuring the server for this particular service, we in no way interfere with nor prevent you from using another dynamic DNS service if you wish. To do so, however, would require some customized configuration on your part.

Mitel Networks Corporation has tested the functionality of these services with our software. However, we accept no liability for any breach of service on their part. A failure on the part of your dynamic DNS service can result in your network becoming temporarily unreachable from the Internet. During these times, your e-mail may be undeliverable.

If your IP address is assigned dynamically and you intend to receive all your e-mail directly (rather than having it stored at an ISP and retrieving it via POP or IMAP), but you decide not to use a dynamic DNS service, you should implement multidrop e-mail as your e-mail solution as this will ensure that no e-mail is misdirected to another IP address (See *Some important notes on Service list D (multidrop mail)* in Chapter 3.)

Note: Dynamic DNS services are not perfect. They merely point hostnames to IP addresses. If your system receives an IP address via DHCP or PPPoE, it will automatically update the dynamic DNS service each time it comes online. However, when your server disconnects from the Internet, with most dynamic DNS services your server does not indicate that it is offline in any way to the dynamic DNS service. If your system is offline for a period of time, it is possible that someone else will be assigned your IP address by your ISP. If this occurs, with most dynamic DNS services this other system will now start receiving your e-mail and web page requests until your server comes back online and updates the service with your new IP address. There is not much you can do about this, but you should be aware of this fact if there is any chance your system will be offline for a long period of time.

Appendix C. Proxy Servers

The server comes with a proxy server called Squid which can proxy the web (HTTP), FTP and Gopher protocols. Proxy servers temporarily store information from the Internet on the hard drive of the server, allowing other users to access it directly from that hard drive. For example, when an employee visits a web page, the web proxy server will store that web page. Subsequent visitors to that web page will read it from your proxy server's hard drive, rather than over the Internet. This slightly reduces the network performance for the first visitor to that web page, but can enhance the performance for subsequent visitors.

Many gateway systems require the use of proxy servers, but with the server it is optional. Networked applications such as web browsers will work perfectly without proxying, due to the IP masquerading capability of the server.

In general, we recommend that proxying be disabled in your network applications. Using the proxy server can benefit the organization if you have a slow Internet connection and you've installed your server software on a fast computer. In this case, reading from the hard drive will be faster than reading from the Internet. Remember, though, that a proxy server benefits the second and subsequent visitors to a site but not the first visitor, so this benefit only applies if your users tend to visit the same sites repeatedly.

A proxy server is generally not appropriate if you have a fast Internet connection and you've installed your server software on a lower- or mid-level computer. In this case, reading from the hard drive of the computer may not be faster than over the Internet. It also offers no benefit to your organization if employees at your site do not tend to visit the same web pages.

Appendix D. Technical Support

If you are a Mitel Networks Corporation subscriber and are having technical difficulty, please contact your local Mitel Networks Corporation authorized reseller for support. If you purchased your subscription directly from Mitel Networks Corporation, please call +1-613-271-7614 (in the United States and Canada, call 1-866-472-9999) and ask for technical support or e-mail us at support@e-smith.com. You can also visit our website <http://www.e-smith.com/>. Please have your server registration number ready when you contact us for support.

If you are having difficulty configuring another vendor's hardware or software, we recommend you refer to the manual or contact the vendor for that product.

As the SME Server V5 is open source software, Mitel Networks Corporation encourages users to freely share copies of our software. However, we can only provide technical support for customers who purchase products. So, if you receive a copy of the SME Server V5 software from another source it is not supported or warranted in any way.

Of course, if you have an unsupported version of the SME Server V5, we are glad you are using our product and would welcome your business! You can purchase a subscription from any Mitel Networks Corporation authorized reseller. For a list of authorized resellers in your area, call 1-888-376-4841 or +1-613-564-8000, or check our web site at <http://www.e-smith.com/>

e-smith.org

Developers may wish to note that additional documentation, including HOWTO documents and a FAQ, can be found on our development web site - <http://www.e-smith.org/>. There are also links there to other web sites relating to the server.